

National Institute for



RISR No. 23/2020

ROMANIAN INTELLIGENCE STUDIES REVIEW



“MIHAI VITEAZUL”
NATIONAL INTELLIGENCE ACADEMY



ROMANIAN INTELLIGENCE STUDIES REVIEW

No. 23/2020

The *Romanian Intelligence Studies Review* is an open access academic journal with scientific prestige, acknowledged by the National Council for the Validation of University Titles, Diplomas and Certificates (CNADTCU), indexed in the international databases CEEOL and EBSCO.
For more information please visit the official website www.rrsi.ro.

**Bucharest
2020**

Advisory Board:

Michael ANDREGG, St. Thomas University, United State of America
Cristian BARNA, “Mihai Viteazul” National Intelligence Academy, Romania
Vasile DÂNCU, “Babeş-Bolyai” University from Cluj, Romania
Ioan DEAC, “Mihai Viteazul” National Intelligence Academy, Romania
Christopher DONNELLY, Institute for Statecraft and Governance, Oxford, Great Britain
Iulian FOTA, “Mihai Viteazul” National Intelligence Academy, Romania
Jan GOLDMAN, New Hampshire University, Great Britain
Cristina IVAN, National Institute for Intelligence Studies, MVNIA Romania
Sergiu MEDAR, “Lucian Blaga” University from Sibiu, Romania
Mark PHYTHIAN, University of Leicester, Great Britain
Elaine PRESSMAN, Netherlands Institute for Forensic Psychiatry and Psychology, Netherlands
Fernando VELASCO FERNANDEZ, Rey Juan Carlos University from Madrid, Spain

Associate reviewers:

Cristian BĂHNĂREANU, Centre for Defence and Security Strategic Studies within “Carol I” National Defence University, Romania
Lars BAERENTZEN, PhD in History and former Intelligence Practitioner within Danish Defence, Denmark
Cristina BOGZEANU, Centre for Defence and Security Strategic Studies within “Carol I” National Defence University, Romania
Ruxandra BULUC, “Carol I” National Defence University, Romania
Ioana CHIȚĂ, “Mihai Viteazul” National Intelligence Academy, Romania
Dacian DUNĂ, Department of International Studies and Contemporary History, University Babeş-Bolyai of Cluj-Napoca, Romania
Claudia IOV, Department of International Studies and Contemporary History, University Babeş-Bolyai of Cluj-Napoca, Romania
Marius LAZĂR, Department of International Studies and Contemporary History, University Babeş-Bolyai of Cluj-Napoca, Romania
Sabina LUCA, “Lucian Blaga” University of Sibiu, Romania
Sabrina MAGRIS, Ecole Universitaire Internationale from Rome, Italy
Cristian NIȚĂ, “Mihai Viteazul” National Intelligence Academy, Romania
Silviu PAICU, “Mihai Viteazul” National Intelligence Academy, Romania
Alexandra POPESCU, University of Bucharest, Romania
Alexandra SARCINSCHI, Centre for Defence and Security Strategic Studies within “Carol I” National Defence University, Romania
Ileana SURDU, National Institute for Intelligence Studies, MVNIA Romania
Bogdan TEODOR, “Mihai Viteazul” National Intelligence Academy, Romania
Andrei VLĂDESCU, National School of Political and Administrative Studies, Romania

Editorial board:

Editor in Chief - Mihaela TEODOR, “Mihai Viteazul” National Intelligence Academy, Romania
Editors - Irena CHIRU, “Mihai Viteazul” National Intelligence Academy, Romania
Florentina HĂHĂIANU, “Mihai Viteazul” National Intelligence Academy, Romania
Valentin NICULA, “Mihai Viteazul” National Intelligence Academy, Romania
Valentin STOIAN, “Mihai Viteazul” National Intelligence Academy, Romania
Cătălin TECUCIANU, “Mihai Viteazul” National Intelligence Academy, Romania
Editorial Secretary and cover - Lucian COROI

CONTENT

INTELLIGENCE ANALYSIS	5
Predrag PAVLIĆEVIĆ Risk of terrorism and analysis of counterterrorism concepts: a viewpoint from Serbia	6
Andrei VLĂDESCU About stereotypes – from typographical moulds to matrixes of thought	32
INTELLIGENCE AND SECURITY IN THE 21ST CENTURY	53
Ioana LEUCEA Intelligence and the IR constructivist approach.....	54
Alexandra POPESCU, Teodora DOBRE Defining Hybrid Warfare – the Russian experience: an analysis of propaganda mechanisms and their importance in developing foreign policy	65
Adrian BARBU Rețeaua de dezinformare „Sputnik” de pe platforma Twitter.....	89
HISTORY AND MEMORY IN INTELLIGENCE	103
Codruț LUCINESCU Soviet Russia and “Hybrid Warfare” against Romania between WW I and WW II	104
SECURITY PARADIGMS IN THE 21ST CENTURY	116
Cristian BARNA, Valentin NICULA Prioritizarea riscurilor și amenințărilor la adresa Securității Naționale a României. O perspectivă transversală 2013-2020.....	117

Valentin STOIAN

Translating the Copenhagen School: a view from Romania..... 150

Caroline GRACE, Jiaming HUANG, James M. KEAGLE

A call to action: responding to Russian Hybrid Warfare..... 172

Ileana Cinziana SURDU

Fake news, ethics and responsibility in media reporting
in case of security threats and sensitive issues.

An empirical research of the practitioners' experiences..... 192

GAMES, EXERCISES AND SIMULATIONS..... 212

Bogdan-Alexandru TEODOR, Mihaela TEODOR

Educație în Intelligence: metoda Wargaming..... 213

REVIEWS AND NOTES..... 222

Simon Sinek, *Liderii mănâncă ultimii: de ce unele echipe
lucrează bine împreună, iar altele nu*, Publica Publishing
House, Bucharest 2014, translated by Gabriel Crețu,
review by Valentin NICULA

223

ACADEMIC FOCUS..... 225

CRESCent Project 226

ARMOUR Project 228

THESEUS PROJECT 230

HYBNET Project 232

CALL FOR PAPER *Romanian Intelligence Studies Review* 234

INTELLIGENCE ANALYSIS

RISK OF TERRORISM AND ANALYSIS OF COUNTERTERRORISM CONCEPTS: A VIEWPOINT FROM SERBIA

Predrag PAVLIĆEVIĆ*

Abstract:

The paper starts from a definition of terrorism which is widely accepted and frequently used in scientific publications in Serbia, due to its compatibility and accuracy. The paper also explores the reasons for adopting such a definition of counterterrorism (CT), which encompasses a wide spectrum of countermeasures, normative frameworks and institutional architectures. In order to fundament the scientific discourse, the concept of risk was examined, as well as indications about an essential element of risk, i.e. the negative consequences for the entity. In the definition of risk, as one of its key elements, the vulnerability of entities is emphasized, which includes their resistance or, to put it differently, their ability to carry out adequate responses. This aspect is highlighted as it confirms the goal of the model of analysing the concept of counterterrorism, but also the deepest basis for the construction of the CT concept. Additionally, some components of the new intelligence paradigms are also highlighted, which may be of relevance for the research of the CT concepts. The paper concludes that the adaptability of the normative and institutional framework is the main objectives of the CT constructions. Adaptability also pertains to action plans and measures to the current threats and must include timely determination of the directions and instruments for action, as well as the establishment of solutions that involve the anticipation of future risks. It has been previously highlighted that the goal of CT is to achieve the coordination of the strategic, tactical, and operational level of activity and provide an innovative, creative and proactive perspective. The key direction in the field of CT is not only to achieve efficiency, but to be effective as well.

Keywords: *risk, terrorism, intelligence, antiterrorism, institutions.*

* PhD, Academy of National Security Belgrade, Republic of Serbia, email: predrag.pavlicevic@yahoo.com

Introduction

Nothing new can be concluded by stating that terrorism is one of the key security challenges and risks for the modern world. That is precisely why, in the present paper, we employ the following definition:

“Contemporary terrorism is a multi-dimensional political phenomenon which can be theoretically and generally defined as: a complex form of organized group, and less individual or institutional, political violence, marked not only by physical and psychological intimidation, but also sophisticated technological methods of political struggle, as a means with which whoever usually, especially during the political and economic crisis and rarely during economic and political stability of the society, systematically attempt to achieve ‘great goals’ in a morbidly spectacular way, inappropriate to certain conditions, such as social situation or historical possibilities of those who practice it as a political strategy.” (Simeunović, 2009, p. 80)

Contemporary terrorism is, therefore, a complex phenomenon through the causes that trigger it and through its forms of manifestation and impact which on both the political, security, military and economic sphere, and on culture, tourism, sport, and ultimately in the everyday life of many people. The complexity of terrorism forces the field of counterterrorism to encompass a wide range of countermeasures with the built normative frameworks and institutional architecture. As a result, the definition of counterterrorism must also be formulated in such a way so as to involve all the aforementioned elements. Likewise, the model for the analysis of counterterrorism concepts needs to include the same aspects. In order to link the indicated issues, we need to first start with a discussion of the concept of risk.

The Concept of Risk

The definitions of risk in modern theory are multiple, and in this paper, we adopt the following definition: “[Security] risk is the possibility of a change of situation within or in connection with a social or political entity expressed through a set of determinants of a different and measurable degree of influence and objective significance that are determined by the character and extent of potentially respectable

negative consequences for the entity depending on the certainty of the occurrence of a particular model of social, or technological processes, as well as the degree of vulnerability of the entity determined by the severity (strength of the influence) of the threatening factors and/or of the potential of the threatening entity to expand opportunities in which it takes advantage of weaknesses of threatened entities and causes them damage, loss or destruction, depending on the extent of possession of capacity, quality and/or specific abilities of endangered entities required to take adequate countermeasures. Security risk therefore includes natural processes of a certain volume, intensity and destructive character, technical and technological destructive events, as well as social processes and circumstances that are registered within or in the environments of entities that indicate the possibility that their development adversely effects on stability and/or the realization of entity functions, i.e. the existence of social and political forces of a certain character and objectives of action that have the capacity to significantly threaten a particular entity or its part.” (Павлићевић, 2017, p. 122)

If P_i denotes a set of functions that represent possible events with negative consequences, R_i is a set of functions that represent the degree of vulnerability of the entity (its potential, its ability to defend itself or to prevent the negative outcomes of events), while u_i denotes the potential of the threatening entity, then the equation of risk is:

$$R = \frac{P_1 + P_2 + \dots + P_n}{R_1^{u_1} + R_2^{u_2} + \dots + R_m^{u_m}}$$

$$R = \frac{\sum_{i=1}^n P_i}{\sum_{j=1}^m R_j^{u_j}}$$

Where:

P_i – probability of occurrence of events with negative consequences, $i = 1, \dots, n, 0 \leq P_i \leq 1$

n – number of possible events with negative consequences

R_j – function of the degree of vulnerability of the endangered entities, $j = 1, \dots, m, 0 \leq R_j \leq 1$

m – the number of vulnerable entities (i.e. the number of locations that can endure damage or injury within an endangered entity)

u_j – the potential of the threatening entity, $j = 1, \dots, m, 0 \leq u_j \leq 1$

Surely, it is necessary to investigate in more depth the validity of the cited definition and the mathematical formula of risk. We consider that a slightly modified version of Павлићевих's definition can be applied for the purpose of this paper. Namely, the vulnerability of the entities is highlighted as a key element of risk, which consists, by definition, of two elements:

1. the resistance of the endangered entity, i.e. its ability to undertake countermeasures (i.e. "the extent of possession of capacity, quality and/or specific abilities" to prevent the negative consequences of events or processes) adequately/proportionately
2. the character and strength of the threatening factors (i.e. the potential of the threatening entity to cause the damage, loss, or destruction of the endangered entity).

The analysis model of the CT concepts shows the importance of the concept of resistance on the part of the endangered entity. Considerations build a theoretical approach in which the definition of a risk field is indirectly determined by the ability to overcome it. In this section, the author gives an indication about another important element of the definition – an element that concerns the negative consequences for the entity. Let us begin with the following stance:

There are, however, good reasons for not restricting the concept of risk to negative consequences and many definitions of risk relate it to both negative and positive consequences. What is a negative consequence or outcome? To some, an outcome can be negative, and for others positive. We wish to avoid a discussion on whether a consequence is classified in the correct category. In an assessment of

risk, the aim is to uncover all relevant consequences, then assess uncertainties and assign probabilities. (Aven, 2009, p. 65)

We agree with Aven's statement according to which "in risk assessment, the aim is to uncover all relevant consequences" (2009). A particular phenomenon (process) is the object of our interest precisely because it has consequences of great importance to people. Therefore, the goal is to judge *which* consequences (i.e. not necessarily negative, but consequences of whatever clear significance) have a certain occurrence or process for the values that the society (the state) protects. However, in understanding risk we must bear in mind that it is a social construct, and so it necessarily contains a value (subjective) dimension. The scope of the term risk (in the sense of the values that it encompasses) cannot be limitless – at least for humans, if not for God or for the universe. Risk is the uncertainty of the change of a given state (of the system) – of such a state where there are certain factors beyond its boundaries, which due to their character (volume, degree, intensity, orientation, strength, quality changes) can endanger the system under its protection (its values) – and just as such factors (as factors with specific influence) become a risk factor. It is necessary to defend the assumption that risk, in the theoretical model or in a specific research project in the field of (national) security, signifies uncertainty of occurrence that may have negative outcomes (or the likelihood of the event or process with the specific characteristics – that may have negative consequences) – because risks disturb the functioning of the system, and the goal is to strike a balance in the system.

Hence, the goal is to judge *whether* a particular event leads to the positive or to the negative outcomes. Then the goal is to determine *to what extent* the outcomes of a phenomenon have negative or positive influences on the value(s) which we protect. Outcomes can be determined only by understanding the given reality through thought models because the data provide a certain quality only in the theoretical framework, the very facts stay as bare facts only. Ergo, if we have not defined the risk as a manifestation and outcomes of phenomena (processes) that are negative for the system, we have placed a sign of equality between the notion of *risk* and that of *challenge* –

because the components which constitute the latter can have a positive and negative direction which might affect the values that we protect.

Likewise, if the risk is not defined in a way that leads to the research of negative outcomes of phenomena and processes – since in the cognitive process the fact of the negative influence exists just for the subject – the subject of the cognitive process is lost. The risk is analysed first and foremost to register the negative influences (of risk factors) for the entity, the level of threat to the values that a society (the state) protects, in order to take countermeasures aimed at reducing risks – including raising the entity's ability to improve its defensive potential. Risk is determined by the context, as well as by the research perspective – whereby the criterion of objectivity of research procedures should not be confused with this starting assumption of risk research. Objectivity is achieved by both qualitative and quantitative methodologies, as it is sometimes stronger when the two are combined.

Aven (2009) also argues that “not restricting the risk concept to negative consequences” may, however, have a different kind of foundation – and when one underlines the importance of the time sequence, period, current state and position of the entity at risk. Namely, the protected values change over time, the negative outcomes can become positive and vice versa. In other words, changes within the system alter both the risk perspective and the risk factors. Therefore, any subsequent risk analysis in the field of (national) security must reconsider its evaluation criteria – otherwise the results will not be the real basis for decision making because they will not follow and anticipate changes. In this regard, taking into account the multifaceted and dynamic nature of political and security phenomena and processes, we can agree with the view that it is necessary to overcome “a discussion on whether a consequence is classified in the correct category” mostly because of the fact that positive outcomes can be latent negative and vice versa.

Counterterrorism

Omelicheva (2007) considers that counterterrorism “in its broadest and fullest sense” involves numerous policy areas and includes the activities of almost all governmental agencies (“not only

those authorized with law-enforcement, intelligence, and defence functions”), and that as a type of policy “encompasses a range of actions (e.g., freezing financial assets of terrorist organizations), specific decisions (e.g. a decision to join international treaties aimed at addressing different aspects of terrorism), general guidelines (provisions allowing for the use of military force on the territory of other states), observable behaviours of states (e.g. police raids on possible terrorist sites), and verbal statements of policy makers (e.g. promises of military and economic aid to other states struggling with terrorism)”. Since “counterterrorism measures do not stop at the borders of the states”, Omelicheva (2007) claims that: “As the threat of terrorism blurs the boundaries between internal and international security, the concept of counterterrorism also blurs the distinction between foreign and domestic policy dimensions”. In other words, the scholar states that “counterterrorism can be thought of as a mix of public and foreign policies designed to limit the actions of terrorist groups and individuals associated with terrorist organizations in an attempt to protect the general public from terrorist violence”.

Stepanova (2003) defends the following approach: “To denote efforts to combat and prevent terrorism, the terms ‘counterterrorism’ and ‘anti-terrorism’ are both used, as they have both become a standard part of the United Nations lexicon. In contrast to some national definitions, notably those suggested by the US military doctrine, ‘counterterrorism’ should not necessarily be viewed as being limited to offensive or active measures to fight terrorism, nor should ‘anti-terrorism’ be used to embrace defensive or passive strategies only. As used in this report, neither of the two terms carries any evaluative connotation. The choice between them is determined by a functional approach: while counterterrorism is seen as a security task performed by the security component of a national or international authority, the use of political, legal, economic, civil society and other peace-building instruments for the purposes of both countering and preventing terrorism is more broadly referred to as anti-terrorism” (Stepanova, 2003, p. 8)

Pavličević (Павлићевић, 2016, pp. 51-52) emphasizes the necessity to respect the requirement for the removal of the value

component in the determination, but if we support the aforementioned opinion without limitation, we might miss the fact that in some texts the term 'counterterrorism' connotate "the use of political, legal, economic, civil society and other peace-building instruments" – that the author defines as anti-terrorism. Since the above function of antiterrorism can also be a function of counterterrorism, Pavličević (2016) concludes that a functional approach carries inconsistencies, and highlights that these terms are not antipodes or antonyms. Pavličević also notes that Stepanova consistently used these terms in the meaning set by her in the text: A) anti-terrorism mainly refers to measures and activities targeted at a specific area (state) and involves preventive measures while B) counterterrorism gets the meanings that contribute to the character of offensive (more aggressive), proactive and repressive strategies (see: Stepanova, p. 17).

Pavličević (2016, pp. 48-56) recalls that modern terrorism is a complex phenomenon and because of that the area of countering terrorism covers a wide set of measures, actions and activities. Pavličević points out that the use of terms related to the conceptual complex of opposing terrorism depends on: theoretical perspective, from the bearer of activities – of the implementers of the measures defined in the fight against terrorism, of the wider social and political framework, historical determinants, then from measures that are considered the content of the concept, i.e. its scope, comprehensiveness and character of measures that are emphasized in the discourse (mark as crucial), as well as the orientation of measures for the specific problems. Pavličević insists on the necessity of the clear and scrupulous language of science and consequently underlines the necessity of the conceptual delimitations in science. Therefore, Pavličević scrutinizes the terms antiterrorism and counterterrorism:

1. *Words antiterrorism (AT) and counterterrorism (CT) can designate different real constructions, doctrines or concepts. Although with close semantic content these terms carry different meanings, whereby the term counterterrorism – in relation to the term antiterrorism – has more semantic content and denotes more active countermeasures (denotes pronounced reaction).* Let us point out, from the English Dictionary (2011,

p. 17, 70 and p. 74): “**anti-** prefix opposed to; against”; **contra-** prefix against; “**counter** adv. contrary; adverse; in an opposite direction; in the wrong way; *adj.* opposed; opposite; *n* a return blow or parry; an answering move; *vti.* to oppose; to retort; to give a return blow; to retaliate”. However, the terms *AT* and *CT* are not antipodes, these two terms do not build a formal-logical dichotomy. In one accepted view, notions build a dichotomy in which two members are positively specified their distinction in sources in the English language is not primarily based on the territorial criterion, but rather according to their purposes, i.e. defensive and/or offensive character of the measures they employ;

2. With regard to the number of sources, antiterrorism is conceptually framed as applying passive (defensive) measures to reduce vulnerability, i.e. the possibility of a terrorist attack (including training, preventive and reactive techniques), while counterterrorism involves the utilization of offensive measures aimed at preventing and reacting to acts of terrorism, primarily by specialized state institutions (trained forces). However, these are not the only determinations, but mostly lexical and referential. Furthermore, *the term counterterrorism has been in use more often in many foreign sources, but is also conceptually wider that it can include antiterrorism* – and in relation to the meaning given to it by some theorists: the system of defensive measures which are undertaken in the territory of the state. Nevertheless, we can note that the term counterterrorism, in some sources, is also used to denote the strategies and activities of states on their territory;
3. It is useful to derive and accept a distinction between *antiterrorism* and *counterterrorism* (and as attributes, for example, antiterrorist legislation) – especially if these terms design a doctrinal setting (as in NATO's doctrine). Namely, mainly in the discourse of the United States (or related to it):
 1. The term *antiterrorism* implies the practice of using intelligence and the reliance on (political, social, psychological) analyses undertaken to anticipate a terrorist attack, essentially

by applying the adequate measures aimed at decreasing the likelihood of an attack on the target by making access difficult, while 2. *Counterterrorism* implies activities that eliminate the threat (including the killing of terrorists), essentially directed at stopping the attack, or by depriving the terrorists of their capability to commit an attack. On this basis (attack vs. defence) one might stress the necessity to separate the aforementioned terms and concepts (the strategies or doctrine that simplifies) – separating is comprehended as prerequisite for an adequate reaction to the surroundings (on the perceived threat), and thus a prerequisite for efficiency¹. It is therefore possible and it is rather customary to denote domestic institutions, resources and armed forces as anti-terrorist – in the sense of “doctrinally, legally and organizationally constructed and empowered to act (defensively) only on the territory of the state”. However, even then there are problems in relation with the exact determination of the meaning of the terms – both because of their content and because of their scopes – since for signifying the abovementioned (antiterrorist) resources, the attribute counterterrorist is used. Part of the answer is that in different countries terminology is used in different meanings (and *vice versa*), so the meanings of the terms overlap and widely vary. It is necessary to advocate respect for terminological differences and conceptual distinctions in the knowledge corpus about the segment of reality. But, the application of the concepts is not provided merely with terminological precision – since the terms by themselves are not the determinations of the phenomena. Also, it is necessary to put certain corpus of knowledge about reality in the relation to the surroundings and to the circumstances. One can conclude, bearing in mind the considered issues, that although the aforementioned concepts

¹ Pavličević (2016, p. 50) refers to: Defining the differences between Anti-terrorism and Counterterrorism?, Discussion in 'Leadership and Professional Development' started by JAB, Sep 14, 2011., http://www.shadowspear.com/vb/threads/defining-the-differences-between-anti-terrorism-and-counterterrorism.1162_3/, accessed on 21.06.2014.

are different because they are basically not identically conceptualized – antiterrorism is aimed at reducing the risk, while counterterrorism is directed at eliminating the threat – the defined activities in both concepts still have the same basic goal: to prevent and suppress, defeat terrorism. In addition, one principle or criterion (for example, in the part of our discourse: attack vs. defence) cannot shape a doctrine, strategy, or policy in any area;

4. *According to its objectives, internal and external measures and activities to counter terrorism – albeit they are diverse in character, content and way of realization – are not conceptually separated.* In particular, diplomatic, intelligence and military measures cannot be separated because the connection between internal and foreign policy in the modern world is pronounced. Nothing can be conceptually separated from legal measures, those that require (new) legal solutions or the implementation of international legal instruments in the internal legal order of the state (e.g. instruments for freezing the financial assets of terrorists, extradition mechanisms). Due to the above, the differentiation of CT and AT measures based on the territorial principle loses its significance;
5. *Intelligence* is a specific component of antiterrorism, and signifies the functioning of the state outside its territory – and on this basis the argumentation falls on the strict distinction between CT and AT measures under the territorial criteria, in particular having in mind the need for cooperation of states in the fight against terrorism. Whereas intelligence agencies are active abroad, it is a matter of counterterrorism – but the data which they provide may be of invaluable significance for the security services and other law enforcement agencies, i.e. in the matters of antiterrorism.

Pavličević concludes that the term *counterterrorism* primarily denotes the realization of planned activities in a given social and political environment (a way of conceiving an adequate reaction, defining an effective response to terrorism, that is, a model of action and a way of achieving set goals), endeavours and efforts, politics,

concrete operations and accompanying processes (trends and consequences), as well as established relationships and connexions (cooperation), achieved results and shaped projects on this basis.

*Thus, counterterrorism primarily carries a developing and dynamic component, but only to some extent. It often refers directly to the very concept, strategy and/or agenda, or simultaneous (national and international) institutions engaged in the fight against terrorism. While for the use of words antiterrorism primarily is important a normative dimension (i.e. again doctrinal framework and strategy) and a static dimension (projection and potential), but once again with regard to the activity aspect because it involves the application of accepted legal and other instruments, resources, defined measures, and techniques shaped in the practice (very often in the meaning of the campaign). Pavličević (2016) believes that the analysis indicates a close interweaving of the meanings of CT and AT and, for the considered subject-matter content (CT policy, strategy, activities, and measures), derives a **synthetic definition**:*

Counterterrorism is a term that denotes a system of both public and confidential (defensive and offensive, proactive and reactive) measures, actions and activities of the state or political and military alliances aimed at protecting themselves and their citizens from terrorism, on the basis of normative principles, guidelines, objectives and strategic priorities of action – including the commitments made through international agreements – with the resources and established institutions responsible for their implementation, in correlation with the political, and based on it, security (and military) concept within the given structure of international relations and manifested (global, regional and local) security trends, geopolitical position and geostrategic interests, as well as the relationships that given political entity build with relevant international actors (Pavličević, 2016, pp. 53-54).

Pavličević (2016) notes that the definition he has formulated is extensive and can be applied in different contexts: it can refer to both offensive and defensive measures, preventive and repressive actions, as well as on the activities undertaken in the country and abroad, on statics and the dynamics of the fight against terrorism – its practical and theoretical aspects – as well as on the activities (and their carriers),

instruments (tools), mechanisms, assets, resources and capacities, methods and techniques, then (strategic, doctrinal) presumption and (planned) objectives in the fight against terrorism. Although Pavličević proposes the use and defines the term *contraterrorism* – which signifies and encompasses counterterrorism and anti-terrorism – due to the reasons expressed in the previous discourse, his approach is not in contrast to the approach of the analysis of the doctrines and practices that strictly separate counterterrorism and antiterrorism. The term counterterrorism with a given conceptual framework has the meaning of the widest model of combating terrorism.

A model for the analysis of counterterrorism

Relying on theoretical and analytical concepts, measures aimed at monitoring the trends of terrorism, on the implementation of instruments, re-conceptualization and assessment of the CT strategy and policy within the EU, i.e. measures of the EU authorities focused on monitoring the development, results and efficiency of the implementation of the defined strategy and policy in the fight against terrorism, that is, with relying on the research of the normative foundations, institutional mechanisms and political determinants of the CT concept EU, Pavličević (Павлићевић, 2012) proposed a model of analysis and evaluation of the concepts of counterterrorism. With the indication that the model cannot be universally applicable² – since there is no single, only one correct and analytically optimal, nor a uniquely efficient organizational model – that is, a model whose settings are aligned with historical traditions, political culture, legal system, specific security challenges and geopolitical position of all political entities. Ergo, the model for the analysis of the concepts of the fight against terrorism encompasses an investigation of the following elements:

² In this paper, the author slightly re-compressed the model, specified and reformulated certain settings from Pavličević (Павлићевић, 2012), but will not refer to sources on the basis of which Pavličević made his viewpoint and conclusions since this would greatly burden the text – but notes that there are several research frameworks, problems and some guidelines were derived from the studies Terrorism, Security and the Rule of Law Project (*TTSRL*).

1. The characteristics and scope of terrorism in political and public discourse, specifically: its intensity and content of the perception of the threat of terrorism, its key marks; the way in which current and potential risks and threats from terrorism in the public sector are defined; compliance of official and media discourse on (counter) terrorism; the determination of the prevailing perspective (military, security, political, legal); the way in which the problem of security challenges, risks and threats is solved; the degree of appreciation of structural factors influencing the trends of terrorism, and how they are followed, investigated and considered;
2. The development of the legal (normative and institutional) framework, respectively:
 - A) Determining the legal documents which regulate the field of the fight against terrorism as well as binding legal solutions in related areas, whereby is necessary to:
 - analyse the normative concept of terrorism, as well as criminal procedural aspects in the (counter) terrorism cases;
 - research whether the strategic directions of operation are clearly defined in the CT normative framework, i.e. whether the postulates, the purposes, the functions and the strategic objectives of the action are clearly defined, and whether they are feasible (whether they can be specified in the action and operational documents);
 - research whether the concept includes the conceptualization of a (political) strategy, a normative and institutional framework for combating against specific and/or significant modalities of terrorist activities: suicide terrorism, lone wolf terrorism, or the abuse of the Internet for terrorist purposes;
 - B) Research whether the CT policy is focused toward the establishment of an adequate and efficient institutional structure, which involves identifying and researching multiple variables, respectively:
 - analysis of the institutional structure, as well as the reasons for the changes (within) of the CT institutional frameworks of the entities, which means: a) determining of (basic) institutions that are directly responsible for the aforementioned security

segment (for CT) in the institutional structure, and b) research on the functionality of institutions whose scope of work among other responsibilities involve the fight against terrorism (their jurisdictions, decisions, scope and degree of implementation of CT measures);

- research whether the functions and powers of authorities and institutions are clearly defined. The aim is to indicate, from the standpoint of their function, their place in the fight against terrorism, which includes a consideration of their structure, composition, tasks, jurisdictions, decision-making procedures and the way of functioning and operation;
- research the way in which the relationships of institutional actors involved in CT activities are established, as well as the principles and forms of coordination in their work, the possibilities and degree of achieving cooperation and communication within the CT system;
- discovering any dysfunctionalities, legal (and operational) gaps, mismatches, elements of indeterminacy (whether there is a lack of precise determining of obligations and responsibilities in the relations of certain institutions in the field of the fight against terrorism), procedural inconsistencies and incompleteness. It is necessary to determine whether the institution CT architecture causes (in some spots) the overlapping of jurisdictions and tasks (caused by the complexity of the normative framework of their activity), the objectives of the work and the responsibilities of institutions, whether the complexity of the process of decision making causes incoherent and inefficient management of activities and initiatives, inadequate coordination, or difficulties in the exchange of information;
- investigate the degree and the way in which it accomplishes coordination with institutions for which CT is not a pre-eminent scope of work;
- having in mind the heterogeneous character of the institutions and organizations involved in CT activities and examine whether their relations and responsibilities are adequately defined, but also whether CT institutions can,

through regular procedures and within clearly defined institutional channels influence on the activities of institutions whose scope of work is not in the first place counterterrorism – whether there is a clear legal basis for their activity, and regulated subordination relationships. In particular, investigate which institutions most often and for what reasons (may) cause uncoordinated and ineffective CT activity, and in which cases, institutions outside the CT structures may inadequately apply established procedures, especially in emergency conditions and situations;

- examine the degree of organizational complexity of the CT institutional structure: check the warnings of the theory that a lot of actors do not mean efficiency, and that it is difficult to rationalize a huge institutional machine if it adequately plays by the principles of preserving bureaucratic power (by continuously striving to justify the requisites of its existence, by expanding its jurisdiction and power). Organizational complexity as a research problem of the CT concept encompasses the analysis of the functional necessity that the jurisdictions of some state bodies, from the standpoint of the needs of the system, also involve the fight against terrorism – including analysis of the degree of institutionalization of their roles as well as their differentiation;
- investigate whether there are established mechanisms, institutions and procedures that function as (effective) control and supervision of CT activity and checking of compliance of activity with normative frameworks – toward defined political strategies and operational tasks –also including respecting civil rights and freedoms.

Other problematic tasks:

1. Investigate the extent to which the network of legal instruments aimed at tackling the problem of terrorism is being upgraded and improved, and to what extent it is a developmental and dynamic concept that expresses the ability of innovation, expansion, readiness of those who implement it to exploit the possibilities of checking the postulates on which it is based. Including the question of

whether it is a concept that seeks to be completed in accordance with the given circumstances and limitations;

2. Research whether the coherence of the CT concept is established at the horizontal level (between different policy areas, in the implementation of defined CT strategy, including the question whether there are differences in the implementation of CT measures by different authorities, in certain problem frameworks) and at the institutional level (and the vertical level, as in the case of the EU). It is therefore necessary to investigate whether the given CT approach brought an end to the principle of integration, conformity of parts;

3. Research whether within the system of institutions whose jurisdiction is counterterrorism (or those to whom it is one of the jurisdictions) by actions of institutions achieve and strive to establish the consistency of measures (by areas, in particular measures of domestic and foreign policy). Previously mentioned include the determination of normative and institutional mechanisms that identify and address problems arising in the alignment of activities in response to a terrorist threat. Also included are problems arising from the lack of or from the insufficiency of implementation of the normative framework. Namely, it is necessary to investigate whether the CT model respects the need of coordination of CT policies in terms of the bound solving of problems and the broadness of the area of activities, and whether the compliance of defined political objectives is achieved;

4. Research whether the conception of the fight against terrorism, at the political level, has a basis in consensus about main and firmed-postulated goals – whether the conception (its instruments) causes conflicts. Cooperation in the security field reflects the degree of compliance and acceptance of political projects (the degree of reaching a political consensus) – that is the reflection and the foundation of the harmonization of legal and operational mechanisms with the political principles and values on which the security (CT) concept is based. Therefore, it is necessary to investigate whether the functional imperative of maintaining normative forms (the stability of value forms) is respected, and therefore the necessary motivation;

5. Research whether the implementation of the normative postulates of the CT strategy and policy strive to respect the principles

of the rule of law and legitimacy, that is, whether CT measures lack legitimacy, whether they suffer from ambiguity and whether they are characterized by indeterminacy;

6. Research whether the CT policy, the nature of the tasks (at strategic, operational and tactical level) and their application are derived from the theoretical assumptions about the phenomenon of terrorism (from several theoretical perspectives). In this regard, whether the CT concept is set up in such a way – and continues to develop on the basis of knowledge of the causes of the problem – that the intention of the CT strategy is not only to resolve and suppress the causes that produce terrorism but also to actively affect them. Likewise, it needs to be emphasized, whether CT concept effects on the environment in order to be proactive;

7. Starting from the utmost importance of the intelligence component, determine how the concept defines the place and role of security and intelligence agencies, and intelligence cooperation: whether in the system there is a precisely defined scope of work of the agencies (determine possible overlaps of jurisdictions, and the need for them), whether coordination of anti-terrorist activities and measures is realized (whether there is a central coordinating body, or a body that deals with the processing, analysis, storage and distribution of data or available information of tactical and/or strategic character), whether clear channels are defined, as well as the principles and rules of inter-agency informing and cooperation, procedures for dealing with crisis situations (a normative framework of responsibility and command, starting from the top of the executive);

8. Research whether the CT model is designed in such a way to effectively respond to the consequences of terrorist activities in order to mitigate them – and to what extent it depends on planned activities (adequately defined tasks, constructed structural assumptions), implementation of operational measures and/or adequate political reactions. Investigate whether the implementation of CT measures includes the deployment of military capacities in *consequence management*;

9. Determine whether the CT concept underlines the need for establishment of external relations, cooperation with partners (with

states, interstate associations, military alliances, international organizations and institutions) in the fight against terrorism, whether strategic partners are defined – degree of cooperation achieved – its basis and frames;

10. Research which (not only financial) resources of institutions have been used in combating terrorism, their scope and characteristics (advantages, disadvantages), as well as to determine the scope, standards and method of using resources;

11. Research whether the CT system seeks to exploit the available resources in related areas, in particular whether it uses mechanisms and instruments used in the fight against organized crime and within crisis management;

12. Research whether the concept requires the construction of a system that aims to achieve the connection of the data system (not only of intelligence), their exchange, timely and adequate use, with full operability and the cooperation of the authorities;

13. Research whether the concept is designed in such a way to provide the basis for continuously completing the legal basis of CT action (decision-making procedures, as well as documents which determine measures and instruments), and align that basis with current processes;

14. investigate whether the concept takes into account the impact of inputs, changed circumstances, new factors of importance for political decision-making and action in the field of counterterrorism, and

15. Research whether the concept is set up in such a way that it continuously gives the opportunity to use the results and proposed bases for decision making that are given in the analyses and reports of the competent institutions and authorities, where this is of particular importance:

- whether the reports include periodic deadlines defined analysis of the development and about the implementation of CT measures, analysis of normative and institutional instruments (including the analysis of the implementation of UN instruments), as well as check the mode of operation. As previously mentioned these require clear criteria for the evaluation and implementation of measures of the CT

strategy, incorporating enough precise and concrete indicators which are the basis for objective, accurate evaluation;

- whether analyses and reports are sufficiently comprehensive, including the whole problem-complexity, that is, whether they cover: analysis of the state, process, achieved results in the fight against terrorism (such as TE-SAT: EU terrorism situation and trend report), recommendations and bases for planning of measures;
- whether the consideration of the elements that are necessary for political decision-making involves the engagement of scientific research institutions (including *think tanks*) in CT programs – in particular for the analysis of the theoretical and doctrinal settings – and to what extent their findings and recommendations are respected.

Focusing on issues of relevance to the practice of counterterrorism implies a systematic framework for considering problems in which a comparative approach should be expressed, and in the research projects:

a) there is improvement of the criteria for the analysis of specific problems of the CT model – (constantly) followed the development of different problems of (counter)terrorism;

b) theoretical approach is compatible with the concept of counterterrorism being investigated;

c) there is research of the interdependence of legal, political and operational measures (whether using the existing instruments or striving for deepening and building of concrete and valid analytical instruments and criteria for analysing the legitimacy and legal basis of CT measures – bearing in mind the postulate of the rule of law, protection of the rights and freedoms of citizens, as well as the development of analytical instruments for international-political aspects of CT policy), but also research about the compliance of measures (by scope and quality) and about the impact and compliance of the CT strategy with policies in other areas, and about the modalities of overcoming and effectiveness of overcoming deficiencies (of measures) and gaps in the legal framework;

- d) critical consideration of the use of techniques;
- e) adequate attention to the analysis of critical infrastructure protection;
- f) the epistemological frameworks of the analysis of the terrorist phenomenon are constantly developing, analysing the trends of the terrorist phenomenon and performing risk analysis.

Components of the new intelligence paradigm and research of counterterrorism

The guidelines for researching the concepts of counterterrorism can surely be complemented. Certainly, guidelines can be supplemented by extrapolation, conceive and/or directly convey just from the settings and elements of the new paradigm of intelligence work – and not only because of the extraordinary importance of the intelligence in the CT concept. It is worth highlighting a few works.

Stănculescu (2105, pp. 19-30) points out that governments must define S.M.A.R.T. policy – which is an acronym for sustainable, manageable, achievable, supported by resources and tangible policy. In this context Stănculescu (2015) examines *Competitive intelligence (CI)*, and recalls that its focus is on selecting, collecting and analysing environmental information in order to produce accurate intelligence products that relate to strategic, tactical, and operational decision-making. The competitive intelligence system should be able to assess the future development – to anticipate events as an integral part of the policy – for that reason it ought to provide reports on historical development, data analysis and alerts that signal problems and possible threats, emphasizing relationships that are hard to notice. The requirement to achieve good results in the application of CI in government agencies is interoperability i.e. compatibility of all information systems, division of specific databases – possible in *governmental cloud*. Cooperation is needed across all segments, with defined access levels. Positive results and the value of CI are manifested if the needs of the decision maker are accurately identified, useful indicators and measures are determined, the problem of data quality is solved, developed technological support for CI, and if the data provision system is easy to utilize.

Mitruş (2015, pp. 9-18) also considers competitive intelligence and, as one of its main functions, determines an early warning of change (risks and vulnerabilities) in the organization's environment. The aim is that the data providing competitive advantages should be linked to the real needs of the state and the outcomes. Mitruş (2015) concludes that the specificities of public sector organizations (hierarchy, budgetary funding, and public accountability) make it difficult to maintain the need for application of C.I. system, but innovative governments can facilitate the acceptance of competitive intelligence programs. We can mark off a type of innovation in the public sector, which Mitruş (2015) mentions – radical change of rationality (the worldview or the mental matrix) – because it seems very significant.

Pavel (2015, pp. 45-56) considers the planning of the intelligence organization's capabilities, emphasizing that it is necessary because of the tasks supporting the management. Change has become a norm – while intelligent organizations are, by definition, the traditional structure, more rigid, and less flexible as they are rooted in the concepts, assumptions and policies of the past. Therefore, it is necessary to strike a balance between change and continuity, pay particular attention to maintaining the values and rules of the organization, the performance and results that are shared in the communication process – that the institutional environment would be predictable and understandable. Strategic documents define values and operational priorities, and must take into account two aspects of the contemporary security environment: 1. Great uncertainty and unpredictability, turbulence, with rapid and deep economic, social, political and technological changes – certainly in the future; 2. Deep policy changes at the organizational level. The purpose of strategic planning is to enable for the organization to achieve results within a global strategy. The organization's strategy must also develop a new concept of performance: “The planning capabilities, based on the conclusions resulted from assessing specific activities will identify and argue for new measurements which will define the set of performance indicators at the organizational level. Along with a communicational process, these new parameters will have to be meaningful to the knowledge workers and to generate ‘commitment’ from them”.

It is necessary to balance the short-term results and long-term progress of the organization³. Also, old solutions cannot be used in a new secure environment – strategy (tactics) must be flexible. Planning offers a holistic point of view (taking into account the complexity of the causes and the consequences that affect the problem), thereby supporting management that has a full perspective, since segments of activities are related. Capacity planning plays an important role in interdependent internal organizational functions, and we highlight the *Monitoring phase outcomes* (piloting, evaluating specific processes). Namely, any improved or new organizational process must first be tested on a small scale. Planning officers offer support for a successful change through monitoring the outcome of organizational pilot projects – the goal is to ensure that the risk of change is small, where to introduce change, how to establish it, and what steps to follow. Also, planning within an intelligence organization ensures compliance, also enables for the organization to get a feedback, and helps create an organizational context. It is necessary to consider plans – because static systems are the most fragile – with adaptation to challenges, quick interpretation of a new requirements within the framework of ongoing action plans that is ensured by identifying objectives at all levels. An intelligent organization must have a sustainable strategy that can achieve quantifiable, measurable targets despite the time and cost constraints. An organization must be designed for the change as a norm, and create a change rather than react to it.

Colibășanu (2015, pp. 57-62) stresses that, both for the private and the government sector, information is increasingly difficult to provide, decisions are made without *sufficient* information, organizations suffer from a lack of sufficient knowledge: “The key word, intrinsic to the intelligence concept: *usefulness*, is gaining even more importance”. Although the expression *useful intelligence* is pleonastic, the data must be in accordance with the needs and wishes of the users. Namely, “*useful intelligence* is the process that transforms data and information (what we know) into actionable knowledge (what we

³ In fact, Pavel (2015, p. 48) presents the key items from: Peter F. Drucker, “Management Challenges for the 21th Century”, HarperCollinsPublishers, Inc., 2000, pp. 44-69.

understand) for decision-makers”, where “The utility of the process is defined by the degree to which it responds, in real time, to the specific need of the organization”. In the context of this paper, we highlight:

- “(...) the *proactive function of the intelligence system* refers to the I (...) focus on the following activities: - identify the vulnerabilities, risks and needs of protection both at the level of the company’s operational systems and global level; - establish and monitor the physical and IT security system protocols...; - monitor, control and revise efficiency of protection measures employed; - adapt protection measures to new needs, new risks and vulnerabilities that may appear; - create a reporting system...”;

- “understanding the external forces... process focuses on the following activities: - establish the specific informational needs for the organization, depending on the relationship and level of dependency on the external players (competition vs. cooperation); - conduct research for information on external players (...);”

- “The environment... coming out of the need for the organization to understand and be able to influence the external environment, with the goal of promoting, supporting its own position... - identify the needs for influence based on the existing dependence links (clients vs. suppliers, potential clients – civil society, etc.)... - monitor the influence activity of the other players and their efficiency (...).”

According to Colibășanu (2015, pp. 68-70) intelligence process and architecture of the intelligence system have to be *inter alia* developed on the following principles: “the architecture needs to ensure that clear missions/goals are being set up for all projects (...) the intelligence department doesn’t need to report ‘everything about the project’, but respond to finite and clear questions. It needs to tell what and why you need to know something (...) take advantage of the knowledge and experience of others (...) provide quick ways to identify the sources of information – documentation analysis is very important (...) retasking function is embedded in the system – it is essential to be able to stop and evaluate after each step (...) final analysis and evaluations needs raise new questions.”

Concluding Remarks

This paper outlines a theoretical perspective that understands (security) risks, and hence the risks of terrorism, through the likelihood of threatening an entity that should be protected from unwanted outcomes of events, processes and trends, in which vulnerability is an essential element of the term – which includes ability, capacities, resources and skills needed to respond to a possible, uncertain threat. Therefore, a model for researching the counterterrorist concept is presented, which – because of assessment for possibilities, even more necessarily, strengthened – complemented by the components of the new intelligence paradigm. The model, in fact, explores the degree to which the ability of the entity to respond to the risks of terrorism, as well as the direct terrorist threat has been heightened. The underlying theoretical approach of our research puts a strong asset on the ability to overcome the risk, because this ability is a response to the potential of the risk carrier needed to collapse the system, and therefore indirectly determines the character and significance of the risk field.

The goals of the CT concept must be the adaptability of the normative and institutional framework, but also achieving the adaptability of action plans and measures according to the current threats – timely defining the directions and instruments of action, as well as the establishment of solutions that involve the identification of future risks. The goal is to achieve the compatibility of the strategic, tactical and operational level of activity – and on such bases an innovative, creative and proactive perspective. Fundamental endeavour in the field of counterterrorism is not to achieve efficiency, but to achieve effectiveness.

References:

1. Aven, Terje, (2009), “Risk Analysis and Management. Basic Concepts and Principles”, *R&RATA* # 1 (12), (Vol.2), pp. 57-73, Available at http://www.gnedenko-forum.org/Journal/2009/012009/RATA_1_2009-08.pdf, accessed on 13.03.2018.

2. Colibășanu, Antonia, (2015), "Building the framework for useful intelligence – The contemporary needs and risks", in *Intelligence in the Knowledge Society: Proceedings of the XXth International Conference*, Bucharest, Editors Niculae Iancu and Irena Chiru, pp. 57-72.

3. *English Dictionary* (2011), concise edition, Webster's Reference Library, Geddes Grosset, Glasgow.

4. Mitruș, Marius, (2015), "Competitive intelligence in the public sector", in *Intelligence in the Knowledge Society: Proceedings of the XXth International Conference*, Bucharest, Editors Niculae Iancu and Irena Chiru, pp. 9-18.

5. Omelicheva, Y. Mariya, (2007), "Counterterrorism: the State of Scholarship, Directions for Future Data Collection and Analysis", *Perspectives on Terrorism*, Volume I, No 2, Available at <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/7/16>, accessed on 12.03.2018.

6. Pavel, Anca, (2015), "Planning for the progress of the intelligence organization in the 21st century", in *Intelligence in the Knowledge Society: Proceedings of the XXth International Conference*, Bucharest, Editors Niculae Iancu and Irena Chiru, pp. 45-56.

7. Павлићевић, Предраг, (2017), "Мигранска криза у Европи и Србија: анализа ризика", *Култура полуса*, год. XIV, посебно издање, стр. 117-134.

8. Павлићевић, Предраг, (2012), "Теоријски оквир за анализу концепата контратероризма ослоњен на истраживање политичких и правних аспеката концепта ЕУ", *Култура полуса*, година IX, бр. 18, pp. 271-291.

9. Павлићевић, Предраг, (2016), "Терминолошки и појмовни комплекс супротстављања тероризму", *Национална безбедност*, Година 3, Број 4/, pp. 25-59.

10. Simeunović, Dragan, (2009), *Terorizam: opšti deo*, Beograd: Pravni fakultet univerziteta (Biblioteka Crimen; 9), Beograd: Dosije studio.

11. Stănciulescu, Virgilius-Traian, (2015), "Smart government: Business/Competitive intelligence, The Key for Decisions in Public Sector", in *Intelligence in the Knowledge Society: Proceedings of the XXth International Conference*, Bucharest, Editors Niculae Iancu and Irena Chiru, pp. 19-30.

12. Stepanova, Ekaterina, (2003), *Anti-terrorism and Peace-building during and After Conflict*, Stockholm International Peace Research Institute, Stockholm, Available at <http://books.sipri.org/files/PP/SIPRIPP02.pdf>, accessed on 12.03.2018.

ABOUT STEREOTYPES – FROM TYPOGRAPHICAL MOULDS TO MATRIXES OF THOUGHT

Andrei VLĂDESCU*

Abstract

From 1798 until now, the society has passed from the term of "stereotype", which at that time called the typographic moulds of lead, to that of "stereotype" in the sense given by Walter Lipmann, that is of the images in our mind, which helps us build an interpretation of the world, necessary to understand it, to adapt and find a place and a role within it.

Although stereotypes seem to play a positive role, helping us to think and react more quickly to a new situation, they are a kind of false friends, leading us to a subjective form of normality, and what lies outside this normality it becomes the fuel for stigmatizing those who are not "common".

Stereotypes contribute to increasing social distance and push people to act to the detriment of other people, such as ethnic stereotypes, those antipathy based on inflexible generalizations, resulting in the emergence of vulnerable communities in the face of aggressive discourses.

The importance of stereotypes as precursors of prejudices and foundations of discrimination is equally great, regardless of whether we talk about the abundance of negative references to Jews in Romanian proverbs and sayings, the negative attributes related to the Roma ethnicity in various Romanian dictionaries, the journalistic discourse related to the "exoticism" of the LGBT community or the unfavourable views of the Hungarian minority by the Romanian majority.

Therefore, conceptions such as "eating at the Jew but not sleeping at night alone in his house" or "they will call the gypsies to take you if you are not behaving yourself" are equivalent to ideas about genetic determination or mental disorder that induce homosexuality, as well as eating meat kept under the saddle by the predecessors of the present times Hungarians and all these ideas are efficient fertilizers for conflicts, waiting only for a trigger.

* PhD student National School of Political and Administrative Studies, Romania, email: andreivladescu@yahoo.com

Keywords: *stereotypes, prejudices, ethnic stereotypes, aggressive public discourse, intolerance, cognitive closure.*

Something about stereotypes

It has been 222 years since Firmin Didot first used the term "stereotype", which at that time named the lead typographic moulds that revolutionized the printing technique. From then until now things have evolved, except that not always in the anticipated directions, at least in terms of the way people perceive and interpret the surrounding reality. And maybe because this is sometimes difficult to understand something, people have simplified the cognitive process, resorting to easier ways of interpreting events and the environment, thus reaching stereotypes within the meaning given by Walter Lipmann, to that "orderly image, more or less consistent of the world, to which our habits, tastes, abilities, comfort and hopes have adapted" (Lipmann, 1922), which is in essence that world we are and feel adapted to, which we understand and it is familiar to us, in which "people and things have their places well known and do certain things expected". Each of us wants to feel "at home" and stereotypes help us.

Concepts that strongly correlate, stereotypes, prejudice and discrimination are faces of the same polyhedron: stereotypes - the cognitive component and often unconscious or involuntary, prejudice - the affective component of stereotypes, and discrimination - the behavioural expression of stereotypes (Devine, 1989). Although stereotypes seem to play a positive role, helping us to quickly form an opinion and adopt a measure as quickly as possible or to have a reaction, they are false friends, which leads us to personal and often subjective forms of normality, and what lies outside this normality and goes beyond the "norms" becomes an argument for stigmatizing those who are not "common" and who are often vulnerable to the power of the "common" majority.

According to some authors, stereotypes are "cognitive filters that capture different characteristics of groups or individuals, some emphasizing them, others ignoring them, depending on context, motivation, affective disposition of the one who processes information" (Stănculescu, 2003). These filters are all the more misleading because

little is known about the degree of accuracy and the substance that composes the various stereotypes (Judd and Park, 1993) and on the other hand their efficiency is determined by the need for *cognitive closure*, that is the desire to identify each problem with a clearly defined solution so that confusion and ambiguity can be avoided (Kruglanski, 1998). This is particularly important because studies show that people with a high level of need for *cognitive closure* easily access their own stereotypes, use them relatively frequently in analyzes and reasoning (Dijksterhuis et al., 1996), and tend to reduce the information seeking time necessary to make a decision (Webster and Kruglanski, 1998).

Sometimes stereotypes are profitable, for example when used to promote a product, to increase or enhance its market value. Often the advertising uses the stereotypes already consolidated in the collective mind: the woman is responsible for the cleanliness of the house and the man provides the financial support for it; the woman prepares the food and the man repairs the stove (although sometimes with risky improvisations, but these are also his concern, because he has the technical knowledge ...); the woman has emotions and the man has rationality; one is admired, and the other is the admirer; one - pink and the other - blue. Mr. Proper helps his **grandmother** to wash the floors more efficiently, Norvea toothpaste comes to the aid of the "**30-year-old man, beautiful, smart and with money**", as for Supramax, it solves the dissensions of the **eternal dyad of son-in-law and mother-in-law**.

However, stereotypes can also complicate things, as they essentially contribute to increasing social distance, raising invisible barriers between communities or pushing people to act to the detriment of other people. This is the case with ethnic stereotypes, which, according to Allport (1956), represent "antipathy based on a wrong and inflexible generalization; the antipathy can be felt or expressed, it can be directed to a group as a whole or to an individual because it is a member of that group". He stated that the ethnic stereotype is "an aversive or hostile attitude towards a person belonging to a group, just because it belongs to that group and is believed to have the intolerable characteristics of the group" (Allport, 1956, as cited in Surdu, 2010).

In the confrontation between in-group and out-group members, stereotypes play an essential role, as they underlie prejudices, which take the form of anti-Semitism when the subject of stereotypes is the Jewish people, of xenophobia when talking about refugees, of homophobia if the references are addressing sexual minorities. That is why we will address in the following some of the stereotypes encountered in the Romanian society, starting from the most vulnerable communities in the face of aggressive discourse: Roma, Jews, Hungarians and LGBT.

Greed + Conspiracy = Jewish?

In the Romanian proverbs and popular sayings there are plenty of references to the Jews (including the well-known word "jidan", a pejorative way of referring the Jews) which is why we believe the assumption that the aversion to the Jews has a considerable temporal extent is justified, being difficult to identify the first moment when it appeared, that "T zero" that can be considered temporal reference: "The Jewish people, daring and devilish"; "At the home of a Jew you can eat, but do not sleep there alone at night"; "To eat in an Yiddish house but to sleep in an Armenian house"; "Boil a Jew and two Greeks come out, boil an Armenian and two Jews come out"; "The red beard jew leads the devil to Easter, the black bearded Jew leads the devil to feed with grass"; "The jew, until he deceives, he does not eat"; "The Jew only from a distance is a man" (we emphasize this saying in particular, since it seems to foreshadow the exclusion of the Jews from humanity itself); "To be worse than a Jew".

Interesting are some unique uses given to the word "jidan" in the Romanian peasant thinking, which denotes the level of intensity with which it refers to the negative characteristics associated with the imaginary Jew: the use, in the popular language of Transylvania and Bucovina, of the word "jidan" for the name given to some insects that secrete a nasty odorous liquid, and in Moldova for the name of a cockroach, the "Mamornic" - *Meloe proscarabeus* (Oişteanu, 2012).

Last but not least, we appreciate that the impact of the Jews on the peasant thinking can be estimated as particularly great, considering the fact that in some geographical areas (among which we mention

Bucovina) traditional characters of the New Year appear as masked characters, and among the masks used there are also those of the anthropomorphized "nasties", which are considered to highlight what is most unpleasant in the human nature, but in a playful way, which allows a free expression, different from that of daily life. These masks include the one that "embodies" the Jews, an element of the set of masks of ethnic character (along with the Turkish, Armenian, Greek and Gypsy masks). The "Jews", as a group of masks, are part of all the participants and play the role of "unscrupulous merchants", one of the strongest stereotypes for Jews.

Coming to the present times, we find from the study "The hate speech in Romania" (Foundation for the Development of Civil Society, 2014) that the themes of the anti-Semitic discourses in Romania are built on the basis of two-dimensional conspiracy theory: the intention of fragmenting the Romanian territory, respectively of economic subjugation of the Romanian people, altogether being "the Judaization of Romania". Thus, if prior to 1919 (when the Jews acquired Romanian citizenship), the foundation of the anti-Semitic ideas was the economic subjugation of the Romanians by the Jews and the attempts to establish a Jewish enclave on Romanian soil, after 1920 the image of the Jewish conspirator of a plan was amplified, in which masonry, capitalism and communism were mixed, and the 1930s were marked by ideas regarding the involvement of Jews in the national losses suffered in World War I. In the 1950s and 1960s anti-Semitic stereotypes were shifted to the image of Israel as an ally of the United States, in the sense of "Jewish capitalist power", and in the national-communist era of the 1970s-80s, the image of the Jew was associated with the violence of the establishment of communism and collectivization, where the fault of the Jews appears to be associated with that of the Hungarians, this theme being so well consolidated that it is maintained even today.

Similar results had a project of monitoring the discursive aggression against Jews and Roma in social media (National Institute for Holocaust Study in Romania "Elie Wiesel", 2016), whose conclusions were that, most commonly, the authors of the aggressive messages mentioned as moral traits of the Jews: greed, immorality, bad intentions, tendency to have criminal behaviour, inferiority to the

Romanians from a spiritual point of view. They also carried anti-Semitic stereotypes from the interwar period (the Jewish innkeeper, pawnbroker or leaseholder), but also theses from the conspiracy space, in two main directions:

- **involvement of Jews in events that marked the history of Romania:** the uprising of 1907¹; the massacre at the White Fountain²; the withdrawal of the Romanian troops after the Soviet ultimatum; the economic crisis of the 1980s; the establishment and maintenance of the communist regimes in Romania and other countries of Eastern Europe (favourite arguments included the belonging to the Jewish ethnic group of Soviet leaders or NKVD leaders and the belonging to the Jewish ethnic group of members of the Communist Party, first or foremost from the secondary / tertiary level);

- **"Jewish plots" on an international scale:** the creation of Islam due to the desire to destroy Byzantine Christianity; the conception, by the Jews of Europe, in the nineteenth and early twentieth centuries, of a project for the establishment of a Jewish state on the territory of today's Romania; conspiracy to remove from power Nicolae Ceaușescu and his execution; the elaboration and application of genocidal policies during World War II and thus of the Holocaust.

One part laziness, one part quarrel and one part thievery make a Gipsy

The "problem" of the Roma people seems to be subsequent to the interwar period, when what stimulated the extremist reflexes was mainly the "problem of the Jews", the Romanian nationalism being rather concerned about this ethnic segment, against the background of

¹ The peasant uprising of 1907 started on February 21st in 1907 in Flamânzi, Botoșani and spread in the following period throughout the country. The uprising was defeated by the Government, its repression by the army leading to many dead and injured people.

² The White Fountain massacre took place on April 1, 1941, in North Bucovina, where between 2000 and 4000 Romanians were killed by Soviet troops as they tried to cross the USSR border into Romania.

the greater visibility, both economically and socio-cultural. As quantitatively (by number) and qualitatively (by the socio-economic positions held) the Roma were not considered "dangerous for the Romanian nation", at that time Romania did not experience an anti-Roma psychosis as one could say that exists now or as it existed against the Jews (Matthew 2010).

Apparently there is no such problem at the moment, if we look at the first EU-MIDIS survey (carried out in 2008 by the European Union Agency for Fundamental Rights in the 27 Member States) that shows that Romania has reported the lowest discrimination level (25%) compared to the Czech Republic (64%) or Hungary (62%). Despite the good score recorded by Romania in this chapter, discrimination exists, and the causes for which the Roma are discriminated against are the marginal, traditional and difficult to integrate character of their community, then the status of fugitives – nomads, customs and beliefs, different from the populations they come in contact with and their perception of their paganism (Surdu, 2010). Another reason for dissatisfaction with the Roma is their behaviour in other countries of the European Union, where they travelled on economic-financial considerations and determined an unfavourable image of Romania and Romanians, which is why there were voices calling for renunciation to the name of "Roma" and the acceptance of the name of "Gypsy", because the resemblance to the word "Romanian" creates confusion that affects the image of Romanians.

The aspect of discrimination faced by the Roma people in Romania cannot be neglected, given the reactions existing within the Romanian society when it comes to this ethnicity, reactions that draw from what we call "peasant wisdom". Thus, one of the strongest stereotypes for the Roma is the criminality (Săftoiu, 2017), more precisely the robbery/theft, accredited by the existence of many proverbs or sayings ("how many gypsies, as much thieves", "the gypsy until they stole they do not live", "it is easy to learn to steal when you live with the gypsies", "he cut his bread with the gypsy's knife", "the gypsy also climbs another's horse"), but also by the phrase "gypsy earning" (which presumes an income slightly illicit, if not really stolen) and verbal derivatives such as "they gypsied me" (equivalent to "I was

robbed/cheated"). The potential danger posed by the Roma results from the warnings issued to non-Roma children, compelled to follow the rules drawn under warnings such as "you will be stolen by the gypsies", "I will leave you to the gypsies", "I will call the gypsies to take you if you are not a good child", "do not go there because you will be beaten by the gypsies". Also a verbal derivative refers to another stereotype related to the idea of Roma people, respectively the one regarding the quarrelsome or noisy behaviour, however disturbing, we think of "gypsy", possibly with a clarifying complement – "as at the door of the gypsy tent" (Săftoiu, 2017).

Other stereotypes suggested by the Romanian proverbs and sayings (Grigore, Neacșu, Furtună, 2007; Săftoiu, 2017) are correlated with violence ("he got used to something as the gypsy horse with the whiplash", "the Gypsy when he became king, first of all he hanged his father"), begging/junk ("if you give something to the gypsy today, he comes also tomorrow", "he asks for dole as the gypsy does", "if flies would make honey, the gypsies eaten with the spoon", "when he is hungry, the gypsy sings/dances"), lack the religious sentiment ("a gypsy is a the gypsy even on Easter day", "only the devil has seen the a gypsy as a pope and weddings on Wednesday"), the marginality ("neither a cask made from an osier, nor the gypsy as a leading man", "nor the reed is not like the tree, nor the gypsy is not like the man"). We emphasize the latter stereotype in particular, because it hides an extra nuance of gravity: not only does it rule the marginal place of the Roma, but prefigures, to the limit, the justification of a violent, perhaps even lethal, action against them.

Moving from the level of the proverbs and sayings to that of the conceptions conveyed in Romania, we found that the thinking has not suffered categorical changes in recent times, at least in terms of the perception on the Roma. Thus, if the results of the "Barometer of Roma inclusion" (Open Society Foundations, 2007) denote vague stereotypes, related to the fact that Roma people identify Roma by the skin colour (23%), appearance/physiognomy (17%) and behaviour (13%), the respondents of the opinion poll "Social cohesion and interethnic climate in Romania" (2008), are much more specific, showing that the main

characteristics that best characterize the Roma are those of "dirty", "thieves" and "lazy", and "most of the Roma are breaking the laws".

Similar were the results of the opinion survey "Stereotypes for the Roma" (Sociological Research and Branding Company, 2010), according to which the most common traits associated with the Roma are: thieves, lazy, filthy, reluctant and backward and, not least, according to a study carried out by the Agency Foundation "Together" in 2013, about 62% of the terms associated with Roma people with Roma are negative, and almost a quarter of them are classified in 3 main categories – theft, laziness and aggression (Cace, Toader, Vizireanu, 2013).

It is possible that a consequence of the way Roma are perceived by non-Roma people is that, according to the opinion survey "Social cohesion and interethnic climate in Romania" (The Centre for Research in Interethnic Relations and The Institute for the Study of the Problems of National Minorities, 2008), 77.9% of Romanians (and 71.9% of Hungarians) have "little" and "very little" confidence in the Roma. Also, another consequence could be that non-Romanians identify a solution to the "Roma problem", a solution that draws attention both through radicalism and its "viability": in 2008, 70.6% of the participants in the opinion survey "Social cohesion and interethnic climate in Romania" thought that Roma should be forced to live separately from the rest of society "because they cannot integrate", an idea found also in 2016, when the solution was deportation somewhere in Romania, in a dedicated area that might allow the detention in safe and controlled conditions (The Foundation for Community Development Agency "Together", 2016).

If you don't have an aquarium it means you are gay

The title above comes from a joke about what reasoning and logic means: if you have an aquarium, it means you like nature, so you like what is beautiful, so you like women, so you're not gay. Otherwise ...

Unlike the previous communities, in the case of the LGBT community, finding the stereotypes through which it is represented in the Romanian collective mind was a real challenge, because a series of elements indicating the "historical" existence and the perpetuation of

the perception were lacking in time, most of them were not demonstrable, more specifically no studies have been identified that analyse the reasons or pretexts that underlie the public opposition to LGBT and neither proverbs or sayings that portray, even caricaturally, the LGBT community, fixing it in this way in the collective memory.

This situation could be explained by the fact that until the last years the LGBT community was practically "out of law" or, at best, not recognized as such, and its members did not benefit from visibility, they were not a recognized part of the society, with their good side and bad side, so that this presence facilitates the appearance of proverbs, sayings, words of spirit, something that defines the community, laudatory or depreciative.

References to LGBT were found in the pages of the Penal Codes rather than in peasant thinking or even "urban literature", as Romanian literature does not abound in homoerotic productions, which is a consequence of the fact that Romanian writers associated homosexuality with something foreign, improper to the Romanian people (Mitchievici, 2010). As a result, gay authors have been marginalized and gay stories censored.

In this regard, we have referred in our approach to "inside" opinions, respectively to the few studies conducted by non-governmental organizations with concerns in the LGBT area, according to which LGBT people are presented as "indecent, provocative, promiscuous or as reversing the roles of gender, while gay men are often associated with transvestites".

Another category of data and also the most of the data collected came from the media, which considered LGBT as an "exotic" topic for the public opinion, perhaps because of the vivid colour of the outfits and the "glamorous" attitude of the participants in the Gay Pride parades. The media attention was not scientific in nature and manifested itself in a somehow unbalanced manner, perhaps even on the background of a limited knowledge of the phenomenon. In this regard, a report monitoring the press, made by the ACCEPT Foundation, submitted between 01.09.2005-28.02.2006 and based on the analysis of a set of articles published in the national newspapers ("Adevărul", "Libertatea", "Ziua", "Evenimentul zilei", "România liberă", "7 Plus" and

“Cotidianul”), noted (especially in tabloid publications) the tendency of journalists to refer especially to gays, while lesbians were much less visible and bisexuals and transsexuals were completely ignored. Also, the attitude of the journalists towards the LGBT community as a whole was generally neutral, although 30% of the monitored articles presented LGBT in a negative way, mainly due to the stereotypes related to criminality, especially paedophilia.

At the level of the journalistic discourse, the ideas conveyed about the members of the LGBT community can be classified according to the following categories:

❖ **the explanation of LGBT emergence / existence**

- they are "sick", homosexuality being a "disease", most often psychic (Ruscior, 2016);
- homosexuality has a biological (Copăceanu, 2017) or genetic determination (National Institute for Mathematical and Biological Synthesis, 2012);
- they were victims of sexual assault in childhood or adolescence (Rotaru, 2019);

❖ **the LGBT identity**

- they dress in bright colours, strident colours (Apostol, 2015), especially pink (Laszlo, 2015);
- they dress in black leather clothes, accessorized with metallic objects (Racoviceanu, 2019);
- they wear clothes usually used of the opposite kind (Bâltoc, 2015);
- gays are the exact opposite of straight men, that means they are not attracted to sports, neither as a practitioner nor as a viewer, they are overly attentive to their "look", they do not have a firm walk, they have feminine gestures, they are interested in cosmetics (Codos, 2015);

❖ **the LGBT behaviour**

- they have promiscuous behavior (Lengyel, 2016);
- they speak affected, in order to obtain emotional expressivity (Pincott, 2017);
- when they are in a group, they become ostentatious (Robu, 2013);

- have non-normative, orgiastic sexual practices (Arvinte, 2017);
 - they consume hallucinogenic substances, especially in the context of sexual acts (Kelland, 2019);
 - gays have female traits and lesbians have male traits (Valentova, Kleisner, Havlíček, 2014);
- ❖ **the consequences of being a LGBT person**
- homosexuals are the cause of the worldwide spread of AIDS (Conrad, 2017);
 - it would not be "normal" that homosexuals constitute a family in the traditional sense of the notion (Tiță, 2017);
 - homosexuality is against nature, because sex has the role of producing children, and homosexuals cannot give birth to children (Dima, 2018);
 - homosexuality is a capital sin (Yedroudj, 2019), which is spreading worldwide (Ionașcu, 2018);
 - if they will adopt a child, he would in turn become a member of the LGBT community (Saiu, 2019).

Az a szep ... but only if he does not think so much about autonomy

The most common stereotypes about Hungarians, encountered in *ad hoc* discussions with Romanians or in the media, refer to the character and nature of Hungarians and their plans (with or without the support of the Hungarian state) to fragment Romania territorially:

- they want to take from us Transylvania or a part of it (Diac, 2017);
- they refuse to speak Romanian, and in the localities with Hungarian majority population if you do not speak Hungarian you are ignored (Dan, 2017);
- they are arrogant and look at the Romanians "from above" (Mut, 2015);

- DAHR³ is an extremist organization (Tănasă, 2015);
- they have exaggerated claims regarding minority rights in the Romanian territory (Lumezeanu, 2011);
 - the autonomy that they request will lead to separatism according to the Kosovo model (Teodoreanu, 2016);
 - they are aliens (Funar, 2019), they came here from Asia by riding horses and ate meat kept under the saddle, in order to be kept eatable (Pârlog, 2009);
 - they are supported by the interference of Hungary in the areas mainly inhabited by Hungarians in Romania (Fati, 2020).

A summary of the defects attributed to the Hungarians was made by Sorin Mitu⁴, who, in the article "Romanians and Hungarians - a nightmare couple", showed that the main accusation of the Romanians towards the Hungarians refers to the "wickedness" – seen as an expression of bullying, followed by "cruelty" – associated with the "primitivism and temperamental character" and with the Asian origin of the Hungarians (Mitu, 2014).

We consider that the mentioned stereotypes must be viewed in the light of the fears encountered at the level of the Romanian society and that were revealed by a series of opinion polls, the most recent being carried out during April - May 2019 by INSCOP Research for LARICS – the Laboratory for the Analysis of the Information War and Strategic Communication:

- 62.6% of respondents agree that “Hungary is acting to gain control over Transylvania, in one form or another”;
- 58.2% consider that “Hungary mixes in an unlawful way in Romania's internal affairs”;

³ DAHR stands for the Democratic Alliance of Hungarians in Romania, the main political organisation representing the ethnic Hungarians of Romania, founded on the 25th of December 1989, immediately after the fall of the Communist dictatorship in the Romanian Revolution of 1989. Officially organised as a national minority organization (not as a party) it nevertheless acts as one of the main parties of Romania. The DAHR has been a parliamentary party since 1990, it has its own representatives in the Senate and in the Chamber of Deputies, and since 1996 was junior coalition partner in several Romanian Governments.

⁴ Professor and director of the Department of Modern History at the “Babeş-Bolyai” University of Cluj, specialist in the history of Transylvania, comparative imagology and the study of nationalism.

- 60.2% believe that “Hungary has the interest for Romania to be a weak state”.

In 2011, the relations between Romanians and Hungarians were perceived favourably, as indicated the results of the “Barometer of interethnic relations” (realized in March 2011 by the Romanian Institute for Evaluation and Strategy – IRES in collaboration with the Romanian Association for Evaluation and Strategy – ARES), according to which 63% of the respondents had a “good and very good” opinion about the ethnic Hungarians. Hungarians were seen as “unfavourable” by 29.8% of Moldova province people, 24.9% of Muntenia province people and 18.9% of Transylvanians and Banat province people. The study also indicated an increased acceptance of this minority among the interviewees: 83% would have accepted Hungarian work colleagues, 79% would have accepted Hungarian neighbours, 80% would have accepted Hungarian friends, and 69% would have been agree to have family members belonging to this minority. A significant detail is the fact that the political representation of Romanians by the Hungarians was accepted only by 46% of the respondents.

The results of the survey are all the more important since, at the time of the survey, the nationalist feelings were freshly marked by an incident centred on a symbol of Romanian history, namely the symbolic hanging, by the Hungarian ethnic Csibi Barna, of a doll that embodied the national hero Avram Iancu, the fact being known by 57% of the respondents in the study, mainly persons over 65 years of age and only 30.8% of the respondents aged between 18-35 years. According to the survey, 70% of the respondents considered that Csibi Barna's initiative would affect the relations between Romanians and Hungarians, and 57% of those interviewed thought that the incident could also affect the relations between Romania and Hungary. In the context of the favourable perception of the Romanians towards the Hungarians, 47% of the respondents stated that Csibi Barna's action “does not represent the opinion of all Hungarians in Romania”, while 45% said that it is “provocative to the Romanians, a gesture of defiance”.

Although the general perception of Romanians about Hungarian ethnicity was “good and very good”, it is worth noting the categorical,

sharp opinions on a number of issues that correlate with some of the above mentioned stereotypes:

- 50% of the respondents had a "bad and very bad" opinion about the possibility of Hungarians from Romania to obtain citizenship of the Hungarian state;
- 72% of the respondents did not agree with the decision of some presidents of the Romanian County Councils to apply for and receive Hungarian citizenship next to the Romanian one;
- 51% of the study participants felt that the DAHR's role in the Romanian policy is a negative one.

Two years later, the "Barometer of public opinion – The Truth about Romania" (survey conducted by INSCOP Research on September 2013), shows that Romanians consider relations with the Hungarian minority in the last place in terms of good relations throughout history (with 27.2% of respondents) in a hierarchy of which the following ethnic minorities still belong: Serbs (69.4%), Germans (69%), Bulgarians (67.9%), Jews (59%), Turks (49.9%), Roma (30.2%). The only minorities to which the respondents mostly considered the relationships have been throughout history are the Roma (58.8% – "bad relations") and the Hungarian one (59.7% – "bad relations").

In the same survey, 29.1% of the respondents consider that the present day relations between Romanians and Hungarians are "bad and very bad", for 29.2% they are "good and very good", and 37.3% evaluate them as being "neither good nor bad". And on this dimension, the difference between the geographical regions is maintained, which can be explained as we have tried above: the residents of Banat-Crișana-Maramureș and Transylvania perceive the Romanian-Hungarian relations as "good and very good" in a proportion higher than those of Moldova-Bucovina and Muntenia-Oltenia-Dobrogea.

What draws attention is that, according to the INSCOP survey, radical opinions and intransigence tend to diminish among people who have contacts (relatives, friends, acquaintances, neighbours) within the Hungarian community:

- of the people who have Hungarian knowledge/ friends, 42.7% consider that the historical relations with the Hungarian minority are "good", while, at the level of those who do not have

Hungarian knowledge, only 16.6% consider the historical relations with the Hungarian minority as "good";

- also, respondents who interact with Hungarians consider to a much greater extent (45.9%) that the present relationships are "good and very good", compared to those without connections in Hungarian environments (19.1%);
- those with Hungarian knowledge consider to a greater extent than those without Hungarian knowledge or friends that Romanian-Hungarian tensions have as substratum "exaggerations of the press" (26.6%, respectively 12.9%), and reciprocally, those without Hungarian acquaintances or friends consider that tensions are caused by "electoral challenges of Romanian and Hungarian politicians".

Conclusions

Ideas such as "eating in the Jew house, but not sleeping there at night" or "gypsies will take you if you are not behaving yourself" compete as intolerance and reductionism with scientifically unsustainable assumptions about genetic determination or mental disorder that would induce homosexuality as well as with the meat-based nutrition kept under the saddle by the Hungarian predecessors of the present times, thus constituting fertilizers of the conflict, waiting for a trigger factor.

From stereotypes to the actionable opposition to a social or ethnic group the distance is not as great as it seems at first sight and may depend on seemingly minor events. The recent reality offers enough examples, if we think only of the case of Ditrau, which, paradoxically, opposed an ethnic minority to another ethnic minority, the latter being characterized by an additional attribute, that its members, refugees from Sri Lanka, were strangers not only in the region, but also on the national territory. We say paradoxically, because in this case we can talk about the interchangeability of roles – a community vulnerable to the aggressive discourse of the majority has in turn become an intolerant and aggressive majority, very close to the limit of transposing facts and stereotypes of thinking into violent deeds.

Referințe:

1. Allport, G. W. (1958). *The Nature of Prejudice*. New York, Doubleday Anchor Books.
2. Angi, D., Bădescu, G., Curt, C.G., Greab, C.G. (2014). *Discursul instigator la ură în România*. Retrieved from http://www.researchgate.net/publication/333811833_Discursul_instigator_la_ura_in_Romania
3. Apostol, M. (2015, 23 mai). *Mars în chiloți pentru egalitate | Așa au înțeles homosexualii și lesbienele să-și ceară drepturile*. In *Libertatea*. Retrieved from <https://www.libertatea.ro/stiri/mars-in-chiloti-pentru-egalitate-asa-au-inteles-homosexualii-si-lesbienele-sa-si-ceara-drepturile-1150673>
4. Arvinte, A. (2017, 5 iulie). *Politia din VATICAN a intrerupt o ORGIE de HOMOSEXUALI în locuința unui cardinal*. In *Evenimentul zilei*. Retrieved from <https://evz.ro/politie-vatican-orgie-homosexuali.html>
5. Bâltoc, O. (2015, 20 aprilie). *Designerul Giorgio Armani, homosexual declarat, critică felul în care se îmbracă unii bărbați gay: „Un bărbat trebuie să fie bărbat, nu contează că e homosexual”*. In *Adevărul*. Retrieved from https://adevarul.ro/life-style/moda/designerul-giorgio-armani-homosexual-declarat-critica-felul-imbraca-unii-barbati-gay-un-barbat-trebuie-barbat-nu-conteaza-e-homosexual-1_5534eb19cfbe376e3558f653/index.html
6. Cace, S., Toader, R., Vizireanu, A. (2013). *Romii din România: de la tap ispășitor la motor de dezvoltare*. Retrieved from <http://agentiaimpreuna.ro/wordpress/wp-content/uploads/2014/08/Romii-din-Romania.-De-la-tap-ispasitor-la-motor-de-dezvoltare.pdf>
7. Codos, B. (2012, 29 martie). *Semne ca iubitul tau este GAY! La cafele*. Retrieved from <https://www.lacafele.ro/semne-ca-iubitul-tau-este-gay/>
8. Copăceanu, M. (2017, 16 mai). *Homosexualitatea e biologică, nu o alegere*. In *Adevărul*. Retrieved from https://adevarul.ro/news/societate/homosexualitatea-e-biologica-nu-alegere-1_591ab3675ab6550cb82564b5/index.html
9. Dan, S. (2017, 4 septembrie). *10.000 de lei amendă de la Protecția Consumatorului pentru Kaufland Odorheiu Secuiesc*. In *România liberă*. Retrieved from <https://romanalibera.ro/actualitate/eveniment/10-000-de-lei-amenda-de-la-protectia-consumatorului-pentru-kaufland-odorheiu-secuiesc--466898>
10. Danish Institute for Human Rights. (2009). *The social situation concerning homophobia and discrimination on grounds of sexual orientation in Romania*. Retrieved from https://fra.europa.eu/sites/default/files/fra_uploads/389-FRA-hdgso-part2-NR_RO.pdf

11. Devine, Patricia G. (1989). *Stereotypes and Prejudice: Their Automatic and Controlled Components*. In *Journal of Personality and Social Psychology*. 56(1), 5-18 Retrieved from https://www.researchgate.net/publication/229067921_Stereotypes_and_Prejudice_Their_Automatic_and_Controlled_Components

12. Diac, M. (2017, 27 aprilie). *Avertisment din partea Academiei Române: Ungaria reîncepe propaganda împotriva României. Transilvănenii n-ar fi dorit Unirea din 1918*. In *România liberă*. Retrieved from <https://romanalibera.ro/actualitate/eveniment/ungaria-reincepe-propaganda-impotriva-romaniei--transilvanenii-n-ar-fi-dorit-unirea-din-1918-447511>

13. Dijksterhuis, A., Van Knippenberg, A., Kruglanski, A. W., & Schaper, C. (1996). Motivated social cognition: Need for closure effects on memory and cognition. *Journal of Experimental Social Psychology*, 32, 254-270.

14. European Union Agency for Fundamental Rights. (2009). *European Union Minorities and Discrimination Survey (EU-MIDIS)*. Retrieved from http://www.edrc.ro/docs/docs/cercetari/EU-MIDIS_ROMA_RO_2008.pdf

15. Fati, S. (2020, 18 februarie). *Ungaria preia din atribuțiile statului român în Transilvania. Interviu cu șeful CNCI, Asztalos Csaba*. In *România liberă*. Retrieved from <https://romania.europalibera.org/a/ungaria-preia-din-atribu%C8%9Bile-statalui-rom%C3%A2n-%C3%AEn-transilvania-interviu-cu-%C8%99eful-cnci-asztalos-csaba/30440009.html>

16. Funar, G. (2019, 29 martie). *Împotriva Poporului Român, împotriva României*. In *Națiunea*. Retrieved from <https://www.ziarulnatiunea.ro/2019/03/29/impotriva-poporului-roman-impotriva-romaniei/>

17. Grigore, D., Neacșu, A., Furtună, A.-N. (2007). *Rromii ... în căutarea stimei de sine*. București, Vanemonde.

18. INSCOP Research. (2013). *Barometrul de opinie publică – Adevărul despre România*. Retrieved from <https://www.inscop.ro/septembrie-2013-romani-si-maghiari/>

19. Judd, Ch. & Park, B. (1993). *The definition and assessment of accuracy in social stereotypes*, in *Psychological Review*, 100, 109-128.

20. Kelland, K. (2019, 12 septembrie). *Gay 'chemsex' is fuelling urban HIV epidemics, AIDS experts warn*. Reuters. Retrieved from <https://www.reuters.com/article/us-health-aids-chemsex/gay-chemsex-is-fuelling-urban-hiv-epidemics-aids-experts-warn-idUSKCN1VX1HF>

21. Kruglanski, A. W. (1998). Motivations for judging and knowing: Implications for causal attributions, in Higgins, E. T., Sorentino, R. M. (1998). *Handbook of motivation and cognition: Foundations of social behavior*, 2, 53-92, New York, Guilford Press.

22. Laszlo, N. (2015, 9 aprilie). *Spune-mi ce culoare porți, ca să-ți spun cât ești de gay. Stil masculin*. Retrieved from <https://www.stilmasculin.ro/spune-mi-ce-culoare-porti-ca-sa-ti-spun-cat-de-gay-esti/>
23. Lengyel, P. (2016, 24 februarie). Homosexualitate la oameni și la alte animale. *PeterLengyel*. Retrieved from <https://peterlengyel.wordpress.com/2016/02/24/homosexualitate-la-oameni-si-la-alte-animale/>
24. Lipmann, W. (2009), *Opinia publică*, București, Comunicare.ro
25. Lumezeanu, L. (2011, 23 iunie). Ambasadorul Ungariei – de ce autonomie si cum au pierdut maghiarii lupta de 700 de ani cu romanii. *Ziare.com*. Retrieved from <http://www.ziare.com/politica/maghiarii/ambasadorul-ungariei-de-ce-autonomie-si-cum-au-pierdut-maghiarii-lupta-de-700-de-ani-cu-romanii-interviu-ziare-com-i-1102853>
26. Matei, P. (2010), Romii în perioada interbelică. Percepții naționaliste, in *Spectrum: cercetări sociale despre romi*, Cluj-Napoca, Editura Institutului pentru Studierea Problemelor Minorităților Naționale, Kriterion.
27. Mitchievici, A. (2010). *Sexualitatea damnată și literatura gay românească*. In *Dilemateca*, V (49), 14–21.
28. Mitu, S. (2014, 27 octombrie). *Românii și maghiarii: un cuplu de coșmar?* In *Sinteza*. Retrieved from <https://www.revistasinteza.ro/romanii-si-maghiarii-un-cuplu-de-cosmar>
- Mut, C. (2015, 7 august). Prejudecăți despre români. *Crișana*. Retrieved from <https://www.crisana.ro/stiri/controverse-14/prejudecati-despre-romani-4928.html>
29. National Institute for Holocaust Study in Romania "Elie Wiesel". (2016). *Discursul instigator la ură împotriva evreilor și romilor în social media*. Retrieved from http://www.inshr-ew.ro/ro/files/proiecte/DIU/DIU_social_media_1.pdf
30. National Institute for Mathematical and Biological Synthesis (NIMBioS). (2012, December 11). Epigenetics may be a critical factor contributing to homosexuality, study suggests. In *ScienceDaily*. Retrieved from www.sciencedaily.com/releases/2012/12/121211083212.htm
31. Oișteanu A. (2001), *Imaginea evreului în cultura română. Studiu de imagologie în context est-central european*, București, Humanitas.
32. Open Society Foundation. (2007). *Barometrul incluziunii romilor*. Retrieved from <http://www.edrc.ro/docs/docs/cercetari/Barometrul-incluziunii-romilor.pdf>
33. Pârlog, N. (2009, 6 decembrie). Hunii – Nomazii care au umilit Roma. *Descoperă.ro*. Retrieved from <https://www.descopera.ro/cultura/4532519-hunii-nomazii-care-au-umilit-roma>

34. Pincott, J. Domnii preferă într-adevăr blondele? Știința din spatele iubirii, sexului și atracției. Editura TREI, București, 2017. Retrieved from https://books.google.ro/books?id=BTeTDwAAQBAJ&pg=PT75&lpq=PT75&dq=homosexuali+vorbesc+pitigaiat&source=bl&ots=_QCfUikmqR&sig=ACfU3U2qCGxD6ieW6O6igvVt1yh32dxAJg&hl=ro&sa=X&ved=2ahUKEwjK06Sl7ODnAhVqk4sKHVB6B3AQ6AEwAHoECAgQAQ#v=onepage&q=homosexuali%20vorbesc%20pitigaiat&f=false
35. Racoviceanu, A. (2019, 13 iunie). Creștin Pride. Eu sunt o călugăriță cu barbă! Și? In *Evenimentul zilei*. Retrieved from <https://evz.ro/pride-comunitate-homosexuali-teatru.html>
36. Robu, D. (2013, 9 iunie). Parada gay in imagini: Constitutie laică, nu mentalitate arhaică!!! *Ziare.com*. Retrieved from <http://www.ziare.com/stiri/gay-fest/parada-gay-in-imagini-constitutie-laica-nu-mentalitate-arhaica-galerie-foto-1240004>
37. Rotaru, P. (2019, 19 iulie). *A fi homosexual nu înseamnă să fii bolnav! Ce se întâmplă, doctore?* Retrieved from <https://www.csid.ro/sex/sexualitate/a-fi-homosexual-nu-inseamna-sa-fii-bolnav-18241874>
38. Ruscior, C. (2016, 6 martie). Studiu ACCEPT: Mulți elevi cred că homosexualitatea este o boală psihică. *RFI Romania*. Retrieved from <https://www.rfi.ro/social-85144-studiu-accept-multi-elevi-cred-ca-homosexualitatea-este-o-boala-psihica>
39. Săftoiu, R. (2017). *Categoria etnică din perspectivă lingvistică*. In *Diacronia*, 5, 1–9, Retrieved from <http://www.diacronia.ro/ro/journal/issue/5/A73/ro/pdf>
40. Sociological Research and Branding Company. (2010). *Stereotipurile la adresa romilor*. Retrieved from http://www.apd.ro/files/comunicate/Sondaj_APD_romi.pdf
41. Stănculescu, E. (2003). *Stereotipurile și vârsta în psihologia socială*, București, Credis.
42. Surdu, L. (2010). *Mecanisme de construcție și deconstrucție a stigmatizării în cazul romilor din România*, in *Calitatea Vieții*. XXI, nr. 1–2, 51–70
43. Tănăsă, D. (2015, 21 aprilie). *Cinci motive pentru care UDMR trebuie considerată o organizație extremistă, șovină și antiromânească!*. In *Națiunea*. Retrieved from <https://www.ziarulnatiunea.ro/2015/04/21/cinci-motive-pentru-care-udmr-este-o-organizatie-extremista-sovina-si-antiromaneasca/>
44. Teodoreanu, D. (2016, 25 octombrie). Incredibil! Primarul din Sf. Gheorghe a amenințat românii din Harghita și Covasna cu „soarta sârbilor din Kosovo”, masacrați de albanezi, iar un lider UDMR l-a apărut în direct la TV. *Evenimentul zilei*. Retrieved from <https://evz.ro/primarul-din-sf-gheorghe-ameninta-romanii-si-este-aparat-de-udmr.html>

45. The Center for Research in Interethnic Relations and The Institute for the Study of the Problems of National Minorities. (2008). *Coeziune socială și climat interetnic în România*. Retrieved from http://www.edrc.ro/docs/docs/cercetari/Coeziune-sociala-si-climat-interetnic_ISPMN-2008.pdf

46. The Foundation for Community Development Agency "Together". (2016). *În căutarea demnității*. Retrieved from http://agentiaimpreuna.ro/wordpress/wp-content/uploads/2016/04/Anti-tiganism_In-cautarea-demnitatii.pdf

47. The Romanian Institute for Evaluation and Strategy, Romanian Association for Evaluation and Strategy. (2011). *Barometrul relațiilor interetnice*, Retrieved from http://www.ires.com.ro/uploads/articole/ires_raport_relatii_intertenice.pdf

48. Valentova, J.V., Kleisner, K., Havlíček, J. *et al.* Shape Differences between the Faces of Homosexual and Heterosexual Men. *Arch Sex Behav* 43, 353–361 (2014).

49. Webster, D. M., Kruglanski, A. W. (1998). *Cognitive and social consequences of the need for cognitive closure*. In *European Review of Social Psychology*, 8, 133–170.

**INTELLIGENCE AND SECURITY
IN THE 21ST CENTURY**

INTELLIGENCE AND THE IR CONSTRUCTIVIST APPROACH

Ioana LEUCEA*

Abstract

There is considerable debate as to how intelligence should be defined. Should a definition include covert action or secrecy as being an important part of the activity? Is it relevant intelligence to be defined as the knowledge and foreknowledge necessary to address the external threats or different risks? The article upholds the idea that defining intelligence, implicitly or explicitly, involves adopting and assuming IR theoretical prepositions and intends to explore the implications of IR constructivist assumptions in defining intelligence. In our opinion, the task of defining intelligence is provocative because it is very difficult to reach an objective definition delineated from subjective views imbued in the author's creeds of the preferable world system. For instance, defining intelligence in terms of agency through which states seek to protect or extend their relative advantage places the author in a political culture of organizing the world in realist perspective, with predefined actors, and reveals the dependence to particular security culture.

IR constructivist approach generates alternative interpretations of world politics therefore defining intelligence through constructivist lenses would lead to new hermeneutics, allowing us to critically interpret the classical definitions of intelligence and envisage the way forward regarding the intelligence reform.

Keywords: *definition, intelligence, IR theory, constructivism, security culture.*

Introducere

There is considerable debate as to how intelligence should be defined. Should a definition include covert action or secrecy as being an important part of the activity? Is it relevant intelligence to be defined as the knowledge and foreknowledge necessary to address the external threats or different risks?

* Associate Professor, "Mihai Viteazul" National Intelligence Academy, email: leucea.ioana@animv.eu

The voices who reject the importance of the topic express their reluctance as regarding the value of theories of intelligence. For instance, Philip Davies (2009, pp. 186 - 187), mentions Huxley's aphorism that science is "organized common sense" and speaks about a "cognitive contagion" regarding the nexus theory-intelligence. Davies starts its study mentioning that "Canadians are fond of saying that when America catches a cold they get the flu" suggesting that the topic, intelligence theory, is not so important as "there are entire fields of inquiry that are effectively entirely without theory". Therefore, the author appreciates that "there is no a priori need" for theorizing intelligence as "there is no a priori need the social sciences to have theory in order to be scientific". Yet, Davies (2009, p. 187) admits after a few lines that "theory is, of course, a hugely ambiguous idea in its own right", acknowledging, in fact, that it is not simple and easy to configure the object of study.

The lack of convergence about how intelligence should be defined and in which terms that might configure the entire spectrum of intelligence activities does not prove that theorizing intelligence it's a waste of time, a literary vagabondage or that has little importance compared to practical activities. We believe that there is nothing more practical than a good theory because a good definition should be able to provide a good security strategy, for instance. Defining intelligence in classical terms like collection and analysis of information says nothing essential for the process of intelligence. Essential would be deciphering the relevant information, a process dependent on certain hermeneutics or frameworks of analysis.

Our intention is to reveal the connection and the dependence of traditional definitions of intelligence to a specific security culture, namely with the IR realist/power politics paradigm, and then to explore in which way the constructivist perspective of the international scene modifies the terms of the mainstream definitions of intelligence.

Definitions of intelligence reflect the realist/power - politics strategic culture

The bulk of definitions of intelligence revolve around key concepts specific to Cold War period and subscribed to the realist

paradigm of International Relations. Having as key terms state activity, secret, foreign entities, actual or potential adversaries, covert actions, counterintelligence and, as methodology, planning, collection, analysis, distribution, the traditional definitions are no longer useful in adapting intelligence organizations to challenges of the post – Cold War international security environment.

Even the majority of academics and practitioners of intelligence agree that the post-Cold War environment is not similar to Cold War period for many reasons, like new types of threats, new actors, transnational issues, effects of the information revolution, the Unholy Trinity – weapons of mass destruction, terrorism, organized crime (Schreier 2010, p. 48), the definitions of intelligence do not reflect the spectacular changes which characterize the current security environment when the contextual complexity means that small inputs can lead to dramatically large consequences.

The importance of defining intelligence derives from the creed that a good definition would be able to orient and organize the activities specific to intelligence organizations. For instance, defining intelligence in terms of reducing uncertainty says nothing about an organizing principle for intelligence. We thought that in order to dismantle the prevalent realist definitions of intelligence it would be a good thing to make an appeal to constructivism, an approach which has targeted the main realist assumptions.

IR Constructivist lenses in perceiving the international security environment

IR Constructivism is mainly a post-Cold War approach to international relations. Constructivism challenges the realist assumptions like the anarchic feature of the international politics, which shapes the realist strategic culture, based on the concept of power, one very much criticized for its counterproductive recommendations (reflected by the security dilemma, power politics, the armaments race, spheres of influence). Alexander Wendt (2006), a well-known constructivist theorist, was the one to attack realism by stating that “anarchy is not an objective feature of the international politics, yet anarchy is what states make of it” (Wendt, 1992). Another

influential book is entitled *World of our Making*, written by Nicholas Onuf (1989), stresses the same idea, that the world is a social construct based on our thoughts and our intersubjective meanings and ideas.

We believe that if the realist assumptions are eliminated, the bulk definitions of intelligence, like those selected for illustration by Mark Phythian (2009, p. 57) become irrelevant or obsolete:

“Intelligence is secret, state activity to understand or influence foreign entities” (Warner, 2007)

“Information relevant to a government’s formulating and implementing policy to further its national security interests and to deal with threats to those interests from actual or potential adversaries.” (Shulsky & Schmitt 2002, p. 1)

“The knowledge – and ideally foreknowledge – sought by nations in response to external threats and to protect their vital interests especially the well-being of their own people.” (Johnson, 1997)

These types of definitions consolidate for instance the neorealism perception of the international scene: neorealism perceives anarchy as an objective feature of the international system and derives the security policy recommendations from that assumption. Understanding intelligence as an instrument for implementing a certain type of security policy it becomes clear that defining intelligence is dependent on a certain strategic culture.

Alexander Wendt has been criticized by other constructivist theoreticians (e.g. Zehfuss, 2006) for using the word ‘states’ in his statements as the constructivist ontology regards institutions, like states, security organizations or other social institutions as nothing more than organized culture, institutionalized meanings. States are not a given, but a social construction, an institutionalized meaning at a certain point in time. States are not a constitutive element of social reality. Constructivist ontology assumes that the scientific objects of study are the prevalent understandings, the representations, the ideas, the culture, norms, and identities shared by people. Therefore education plays an important role in shaping who we are as individuals, as members of a certain political community, as citizens of a state or as world citizens.

Constructivism can be perceived as a new ontology, a new epistemology and a new methodology in social sciences in general, and in International Relations as well. As a new ontology, constructivism assumes as objects of study the intersubjective understandings, representations, way of thinking, ideas, mentalities. As a new epistemology, constructivism generates “how possible” type questions instead of “why”, “explanatory” questions and reveals the conditions and the discursive practices that construct a security agenda (Leucea, 2012).

For instance, poststructuralist theories generate critiques aimed at exposing assumptions underpinning states of affairs that have come to be regarded as natural or inevitable, thereby demonstrating that in fact they are not, and drawing attention to the relationship between power and knowledge in the process. As explained by Michel Foucault (1988, 154, *apud*. Phythian 2009, p. 64), “a critique is not a matter of saying that things are not right as they are. It is a matter of pointing out on what kinds of assumptions, what kinds of familiar, unchallenged, unconsidered modes of thought the practices that we accept rest. Criticism is a matter of flushing out that thought and trying to change it. To show that things are not as self-evident as one believed”.

We think that must free ourselves from the realist overarching model of conceiving intelligence, to dismantle and blow up the realist *dictu`* and perceive recommendation like “avoiding the politicization trap” as dependent to a specific strategic and intelligence culture but not unchangeable. Realizing that intelligence “is not simply an objective eye seeing and describing reality but one which participates in the creation and reproduction of a specific international political reality” and therefore, “does not merely describe the world in which the state operates, but in fact actively creates that world” (Fry and Hochstein, 1993, p. 23, *apud*. Phythian, 2009, p. 65) would enable major transformations in designing intelligence in order to better address the future challenges. Understanding intelligence organizations as designed to find and tailor the “best truth” for decision – makers (Bertkowitz & Goodman, 2000) gives little space for improvements. The acceptance of the realist logic is based on the positivist assumptions.

Practitioners are would not be receptive to constructivist approaches of intelligence as long as they believe that the main role of intelligence should be that of telling the “truth to power” and to provide objective analysis, to tailor analysis to match the real or imagined customer preferences. From a realist, traditional perspective, the intelligence services should serve the needs of the policymakers and not to interfere by advocating specific policies. Conceiving in that fashion the role of intelligence, the role is limited, something similar to library services.

Politicizing intelligence in a constructivist perspective

The topic of politicizing intelligence is very much present on the agenda of Intelligence Studies. The recurrent question is whether policy shapes intelligence or the intelligence shapes policies?

Policies specific to Cold War period clearly shaped intelligence, starting with the definition, the role and its objectives. The power politics paradigm limited the intelligence activity, at least during the Cold War period, mainly to statistics, to “counting beans” (Lowenthal, 2009, p. 235). The puzzle of the strategic politics was not put into question. In the post – Cold War international period the puzzle or the strategic map is put into question, as well the defining purpose of the intelligence, that of informing the government – “telling best truth to power”, “producing that particular knowledge that a state must possess regarding the strategic environment, other states, and hostile non-state actors to assure itself that its cause will not suffer nor its undertakings fail because its statesmen and soldiers plan, decide, and act in ignorance” (Schreier 2010, p. 23).

We can state that the politicization of intelligence starts, in fact, with its definition. Adopting a definition like “intelligence is production of unbiased information about risks, dangers and threats to the national vision, and chances or opportunities for the advancement of national interests” (Schreier, 2010, p. 23) we enter in an uncritically accepted bias or, to express it more metaphorically, we enter unprepared into the uncharted waters of the XXI century.

Nowadays, taking into consideration the complexity of the international security environment, the quest for policy relevance of

intelligence products is challenging the Red Line between Intelligence and Policy. Robert Jervis (1986, p. 39) noticed that intelligence is easier to keep pure when it is irrelevant. To be useful, intelligence must engage policymaker's concerns. The traditional conception of maintaining the divide between intelligence and policy can hardly be sustained in a world where we have more mysteries than puzzles (Schreier 2010, p. 55) and where the security threats are terrifying.

The 21st Century Security environment leaves the intelligence communities in the position of not knowing how to prioritize its efforts. Highlighting that "analysis has to move from analysing what is collected to analysing what to collect" (Schreier, 2010, p. 151), yet that was the traditional task of decision-makers, the specialists raise the question of the dividing line, the red Line between Intelligence and Policy.

But if we redefine, for instance, strategic intelligence by stating that it is a process, a means to an end and that end is security; the question that remains unanswered is what justifies the means when they fail to provide security? Should the decision-maker be blamed for intelligence failure or should the intelligence services be blamed for failing accomplishing its task of providing security? This is a serious question and a reason why intelligence failure is a core issue in intelligence studies.

The traditional model of describing the intelligence process does not consider the political factor as being a part of the intelligence cycle. "The intelligence cycle, a model that describes the sequence of activities that carries intelligence from the initial planning stages all the way to a finished product ready for the consideration, consists of five phases: planning and direction, collection, processing, production and analysis, and dissemination. Conceptually the cycle provides at least a rough approximation of how intelligence professionals think of their work." (Johnson 2009, p. 34) The phases of the intelligence cycle do not include the first phase, the most important one, establishing the intelligence needs and priorities, the traditional task of the decision - makers, the configurators of the big puzzle in mapping security challenges.

Conclusions

In other words, as Warner (2009, p. 16), remarks, “intelligence seems to mean roughly what it meant a long time ago. We still use it to denote (among other things) a counsellor to sovereign power, a type of privileged information, and the activity of acquiring, producing, and possibly acting on that information. What we can say without hesitation is that, for most of history, intelligence has been used to oppress and to maintain systems of oppression”.

The prevalent model of conceiving intelligence uses methodological terms: collection-and-analysis, along with counterintelligence and covert action, but leaves aside the relationship between the producer of intelligence and the consumer of intelligence. Although some specialists expressed that “the concept of intelligence cycle prevents an intelligence system from thinking, that analysis and collection are not two different activities, but two names for the same search for knowledge” there are no signs of a revolutionary change in reconfiguring intelligence in accordance with the revolutionary change that took place in the world.

Constructivism raises the awareness towards the importance of ideas, identities, and international political culture and towards reframing the big picture for studying the world, implicitly the intelligence processes.

In conceiving the intelligence cycle, for instance, by placing the analysis first and then the collection phase, the move would reduce the emphasis on surveillance and would accentuate the role of the analyst elevating the role of education in configuring the frames of mind. The target – centric approach does not offer a comprehensive picture for understanding macro dynamics or the grand strategy of the enemy. Focusing on a specific target, more information collected is not the recipe for the correct interpretation. As Richard Heuer (1999, p. 51) highlights by addressing the question: do we really need more information? More information means more understanding? The difficulties associated with intelligence analysis are often attributed to the inadequacy of available information, yet investing heavily in improved intelligence collection systems, comparatively with the small

sums devoted to enhancing analytical resources, improving analytical methods, or “gaining better understanding of the cognitive processes involved in making analytical judgments” might be the key in preventing the intelligence failures. The provocative issue is, in fact, “seeing the elephant” or “seeing the invisible” and not pieces of it.

Estimating the international security environment is dependent on the analyst mind, framework of interpretation. Within the social sciences domain has been accredited the idea that most specialists lack a general perspective, a systemic perspective. It is important to recognize, stresses Buzan & Little (2009, p. 57), that the systemic perspective is created by the analyst. Amassing information would just hide the priority to conceptualize the map, the bigger picture.

Therefore, in order to uphold that for instance secrecy is a key to understanding the essence of intelligence one must clarify the big picture which advocates the definition. If we come to realize that the main task of intelligence should be education, research, creation of a new security culture, then we’ll have an inverted pyramid: more researchers and educators and less collectors. Understanding that “analysing what to collect” comes first places us within the field of Security Studies and International Relation theory. The analyst – centric approach of the intelligence cycle emphasizes the necessity of understanding the intelligence organizations as preeminent learning organizations and research centres, consultative groups of experts.

Among the aims of the Intelligence Studies we find the desiderata to search for a scientific definition of intelligence in order to find as well a good strategy to navigate in the new turbulent international context. Maybe it is necessary that intelligence to have as main role to conceive and establish that strategic culture or the conditions in which threats are eliminated or kept at a distance. The intelligence services could have as well the role to enhance the intelligence education, to promote and create an improved security culture, to build a new security paradigm, to increase the number of intelligence researchers, to extend the educational programs or to develop independent research agenda in intelligence studies.

References:

1. Bertkowitz, Bruce & Allan Goodman, (2000), *Best Truth. Intelligence in the Information Age*, Yale University Press, New Haven and London.
2. Buzan, Barry și Richard Little, (2009), *Sistemele internaționale în istoria lumii*, Polirom, Iași.
3. Davies, Philip, (2009), "Theory and intelligence reconsidered" in Gill, Peter, Stephen Marrin & Mark Phythian, *Intelligence Theory. Key questions and debates*, Routledge, London & New York.
4. Foucault, Michel, (1988), *Politics, Philosophy and Culture: Interviews and Other Writings 1977-1984*, London, Routledge, pp. 154-155.
5. Fry, Michael and Miles Hochstein, (1993), "Epistemic Communities: Intelligence Studies and International Relations", *Intelligence and National Security*, Vol. 8 No. 3, p. 25.
6. Heurer, Richards, (1999), *The Psychology of Intelligence Analysis*, Centre for the Study of Intelligence, Central Intelligence Agency.
7. Jervis, Robert, (1986), "What's wrong with the Intelligence Process?" *International Journal of Intelligence and Counterintelligence* 1, no. 1.
8. Johnson, Loch, (1997), "Intelligence", in Bruce, W. Jentleson and Thomas, G. Paterson (eds.), *Encyclopedia of US Foreign Relations*, New York: Oxford University Press, pp. 365-73.
9. Johnson, Loch, (2009), "Sketches for a theory of strategic intelligence" in Gill, Peter, Stephen Marrin & Mark Phythian, *Intelligence Theory. Key questions and debates*, Routledge, London & New York.
10. Leucea, Ioana, (2012), *Constructivism și securitate umană*, Ed. Institutul European, Iași.
11. Lowenthal, Mark, (2009), *Intelligence. From Secrets to Policy*, CQ Press, Washington, DC.
12. Onuf, Nicholas, (1989), *World of Our Making*, University of South Carolina Press, Columbia.
13. Phythian, Mark, (2009), "Intelligence theory and theories of international relations. Shared world or separate worlds?" in Gill, Peter, Stephen Marrin & Mark Phythian, *Intelligence Theory. Key questions and debates*, Routledge, London & New York, 2009.
14. Schreier, Fred, (2010), *Transforming Intelligence Services. Making them Smarter, More Agile, More Effective and More Efficient*, Study Group Information, Schutz & Hilfe, Vienna and Geneva.
15. Shulsky, Abram and Gary J. Schmitt, (2002), *Silent Warfare: Understanding the World of Intelligence*, Washington, DC, Potomac Books.

16. Warner, Michael, (2009), "Intelligence as risk shifting" in Gill, Peter, Stephen Marrin & Mark Phythian, *Intelligence Theory. Key Questions and Debates*, Routledge, London & New York.

17. Warner, Michael, (2002), "Wanted: A Definition of Intelligence", *Studies in Intelligence* Vol. 46, No. 3, www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html accessed 18 October 2007.

18. Wendt, Alexander, (1992), "Anarchy is what states make of it: the social construction of power politics", *International Organization*, (46), 391 - 426, in Paul Viotti & Mark Kauppi, *International Relations Theory. Realism, Pluralism, Globalism, and Beyond* (3e), Allyn and Bacon, Boston - London - Toronto, 1999, pp. 434 - 459.

19. Wendt, Alexander, (2006), *Social Theory of International Politics*, Cambridge University Press, Cambridge.

20. Zehfuss, Maja, (2006), "Constructivism and identity: a dangerous liaison" in Guzzini, Stefano, and Anna Leander, *Constructivism and International Relations. Wendt and his Critics*, Routledge, London and New York.

**DEFINING HYBRID WARFARE. THE RUSSIAN EXPERIENCE:
AN ANALYSIS OF PROPAGANDA MECHANISMS
AND THEIR IMPORTANCE IN DEVELOPING FOREIGN POLICY**

Alexandra POPESCU*, Teodora DOBRE*

Abstract

In the past few years, the Russian Federation has become a central point on the security agenda of the most important international actors due to its aggressive foreign policy, proven by its latest actions (the illegitimate annexation of Crimea, the actions conducted in Syria and so on). However, by comparison with the Cold War era, Russia has developed new mechanisms to gain power and influence on regional and international level, demonstrating that it can and has the willingness to become the powerful actor that used to be before the Cold War and the fall of the Communist Block by building an empire able to stop the expansion of the North-Atlantic Treaty Organization. Thus, the aim of this paper is to analyse (through instruments like discourse and content analysis and literature review) the methods used by the Russian state to conduct remote wars, without taking responsibility for its actions. Moreover, the article will try to identify the role of the Russian propaganda machine in developing Kremlin's foreign policy, as well as in defining the concept of hybrid warfare as a new form of confrontation.

Keywords: *hybrid warfare, propaganda, disinformation, foreign policy, Russian Federation.*

Motto: *"Social media has evolved. Once considered as a platform for democratic dialogue and deliberation, civic engagement and expression of political ideas, today it has become an instrument of mass manipulation, suppression of votes and of*

* PhD student, Bucharest University and Junior Researcher, "Mihai Viteazul" National Intelligence Academy, email: popescu.alexandra@animv.eu

* PhD student, Bucharest University and Junior Researcher, "Mihai Viteazul" National Intelligence Academy, email: dobre.teodora@animv.eu

propagation of false or tendentious information. Several categories of political actors, from authoritarian governments to Islamist extremists and traditional political parties have efficiently used social media to stifle important political debates, to make reports seem vague, to exacerbate divisions and to block consensus in identifying a response to various public crises". (Bradshaw & Howard, 2018, p. 16)

Defining hybrid warfare

The concept of hybrid warfare took the road of success in the last decades, becoming a recurrent subject on the security agendas of many international actors and organizations. The first advocates of this topic considered that hybrid warfare was defined as a blend of insurgency and conventional warfare, characterized by the use of new technologies, new clandestine methods or the actions of new actors, operating below the thresholds that could define armed conflict (Johnson, 2017, p. 3). In the same line, Hoffman claimed that hybrid wars are a "mixed form of the lethal characteristic of state conflict with the fanatical and protracted fervour of irregular warfare, where adversaries (represented by states, state-sponsored groups, or self-funded actors) take advantage of their access to modern military capabilities, while promoting extensive insurgencies by using ambushes, improvised explosive devices (IEDs), and coercive assassinations" (Hoffman, 2009, p. 37):

"A hybrid war is any adversary that simultaneously employs a tailored mix of conventional weapons, irregular tactics, terrorism, and criminal behaviour in the same time and battle space to obtain their political objectives" (Hoffman, 2014).

The hybrid warfare concept is not considered to be of recent history, however, making reference to the same types of war, but with a far more extended complexity, hybrid forces being able to "effectively adopt and include up-to-date technological systems into their force structure and strategy and to exploit these systems beyond the intended employment parameters" (Nemeth, 2002, p. 74). Theoreticians argued that one of the main objectives of the hybrid war package follows to force any enemy to be compliant to the will of its

adversary, thus combining methods of attack designed to fulfil easily identifiable political 'ends', aspects familiar to scholars of classical war theory (Gat, 2001).

In this context, from a historical point of view, the concept of hybrid conflict came into circulation in order to define a new reality of the conflict between state and non-state actors, a conflict that began to run beyond the commonly agreed principles of the classic war, throughout a series of practices considered to be innovative. Thus, to understand the paradigm shift that the hybrid conflict brings to the configuration and negotiation of power capital in the twenty first century, one must first understand what its precursors are.

Classic conflict/war has been defined on a modern basis at the beginning of the nineteenth century by political philosopher and gunman Carl von Clausewitz, in his work, that later become a landmark in conflict studies, entitled "On War". Clausewitz proposed that war should be understood as a mere continuation of politics by other means. For the Prussian philosopher, war was a form of instrumentalisation of violence under the sign of state power and law, whose goal, most rationally, was to force the adversary to carry out what the subject wanted. Therefore, the conflict came out of the sphere of biological violence and was ethically regulated, becoming a morally accepted form of maintaining/accumulating state power. The ultimate goal of the war, understood in this manner, was not the destruction, but the disarmament of the opponent or the wear of its resources to the point where it could be subjected to its own will (Clausewitz, 2013).

Addressing the conflict as a form of attrition of the enemy's forces, without the actual destruction of the army or the conquest of its territories, the concept of war was later defined by tactics of the asymmetric war, by those agents of power who did not have the same military, political, financial and territorial strength as its opponent.

In the twentieth century, the **asymmetric warfare** approach was developed and refined – a term derived from the Clausewitz's advanced concept of people's war. This evolution had as a starting point the inclusion, in addition to the classic form of confrontation between two armies, of the guerrilla confrontation for the oppression of the opponent. The new type of war that combines the two types of tactics

has been called irregular war. In this manner, the idea of asymmetric war was further developed from the concept of irregular war. The first theorists of this concept were Karl Marx, Friederich Engles, T.E. Lawrence, Mao Zedong, and Vladimir Lenin, who introduced the idea of developing tactical warfare through the instrumentalisation of popular revolts (Engels, 1949), as well as an army of assuring a working class, a political assassination, and a propaganda to strengthen the morale of their own troops and to undermine the adverse forces (Lenin, 1965).

At the end of the twentieth century and the beginning of the twenty first century, we witnessed a new conceptual mutation by the introduction of a new term – that of *hybrid war*, which initially referred to a type of war developed through the synchronized, flexible and well-coordinated use of operations specific to the classic warfare, combined with guerrilla actions, information operations, and the use of advanced technologies. W. J. Nemeth, one of the first authors who spoke about hybrid war, uses this term to describe the war between the Chechens and the Russian forces. In Nemeth's sense, this type of war meant *“involving the whole society and combining conventional war tactics with irregular warfare tactics, as well as information operations that used in an innovator manner modern technology”* (Racz, 2015, p. 30).

The concept of *“hybrid warfare”* saw afterwards a prolific evolution, being usually invoked and refined as to refer to a whole series of conflicts, from the Vietnam War, to the war in Afghanistan, Iraq or Lebanon. In essence, hybrid warfare had been defined as any form of war that incorporates an extensive range of modern instruments, that uses in a fluid manner and well-synchronized tactics specific to various forms of conflict, that act both directly and indirectly in the confrontation area, in order to maintain the adherence and support of its own citizens and the international community, and to weaken the morale and efficiency of target audiences in the area considered to be adversary. Furthermore, Russel W. Glenn offered a new dimension to this concept, making it to incorporate actions in the economic and social area (Glenn, 2009), while Margaret Bond further expanded the dimensions of the hybrid warfare to include *“all elements of national power, through a continuum of activities, from those designed*

to ensure/undermine stability and security, to reconstruction operations, to armed confrontation” (Bond, 2007, p. 4).

To sum up, it is true to say that the term hybrid warfare demonstrates an excess of contextual characterization and an inadequate conceptual clarification, any new instrument, social behaviour or practical use of new technologies offering another element to describe a set of confrontational and competitive approaches, which will certainly define, in time, a new form of conflict approach. For now, however, Russel W. Glenn was right by saying that in defining the hybrid war, the use of metaphors is welcome:

“The best-known hybrid in the animal world is the mule, the product of a horse and donkey. The mule is sterile; it cannot by itself evolve. One must study the evolution of horses and donkeys to understand the potential nature of future mules. The metaphor holds true for the study of what are being labelled hybrid conflicts. The new term may help inspire debate and a better understanding of modern warfare much as did «indirect approach» for some. However, hybrid conflict is ultimately a concept whose character is better described in terms of other constructs that offer superior clarity and will be better understood by students of conflict. «Hybrid» in its several forms fails to clear the high hurdle and therefore should not attain status as part of formal doctrine” (Glenn, 2009).

Even though the specific literature has not managed to identify and develop a mutual definition of this concept, the following understanding can, however, be quite comprehensive:

“Hybrid conflicts...are full spectrum wars with both physical and conceptual dimensions: the former, a struggle against an armed enemy and the latter, a wider struggle for control and support of the combat zone’s indigenous population, the support of the home fronts of the intervening nations, and the support of the international community...To secure and stabilize the indigenous population, the intervening forces must immediately rebuild or restore security, essential services, local government, self-defence forces and essential elements of the economy” (McCuen, 2008; Kanwal, 2018, p. 16).

Therefore, hybrid wars are based on mixed tactics and strategies resulted from combining instruments of both hard and soft power, fact

that allows an actor to obtain the desired results with less effort, by conducting actions that are difficult to track back. With the various extensive effects of globalization and the large development of technology that permitted states to develop a set of instruments which can be used in multiple state areas/domains, avoiding formal commitment of the state into the official war (Banasik, 2015, p. 23), it is true to say that the new form of war exceeds the borders of traditional war, being predominantly based on military operations directly on the ground.

One of the most common non-military means used nowadays by states to project their power/influence against their declared adversaries is represented by information operations, which can be defined as a form of political warfare, where targets include besides a nation state's government, military, private sector, and general population (Theohary, 2018, p. 1). In this context, traditional and social media remain the main mechanism used by a state to target a large audience, playing, at the same time, the role of practical instruments for information operations. With technology becoming a crucial element in the existence of a society, propaganda, disinformation and fake news become a must have asset in a state's portfolio, not necessarily for offensive purposes, but mainly for being able to defend from the offensive actions against the state.

Russian Foreign Policy – Propaganda Mechanisms and Tools

Motto: *“The rules are simple: they lie to us, we know they're lying, they know we know they're lying, but they keep lying to us, and we keep pretending to believe them”.* Elena Gorokhova, *A Mountain of Crumbs* (2010)

The concept of hybrid warfare came to the attention of the main actors of the international scene and of the general public, at national level, with Kyiv's EuroMaidan in late 2013 and the Russian occupation of the Crimean Peninsula in 2014, where the international scene considered that Russia forces have successfully combined psychological warfare instruments with deception operations, skilful internal communication mechanisms, intimidation and media propaganda in

order to avoid direct confrontation and make a favourable context to be able to deny its interference (Tulak, 2009, p. 35).

However, this is not the first case when the Russian Federation used information operations to achieve its objectives, this country being considered a historical past master of disinformation. From the myth of the Potemkin villages, that dates back to 1787, when Russia constructed hollow façades of villages to impress the delegation consisting of European diplomats and demonstrate the success of Russian power and civilization in colonizing the new imperial lands¹ (David-Fox), to the 2001 textbooks episode, when the entire Russian government was convened to analyse the content of textbooks and teacher's books on contemporary Russian history (Snegovaya, 2018, pp. 2-3), concluding that the "*many negative descriptions that appeared in textbooks in the 1990s should be replaced by a vision of Russian history that promotes the strengthening of patriotism, citizenship, national self-consciousness, and historical optimism*" (Butterfield & Levintova, 2009), and to the 2007 "*Munich speech*" of Vladimir Putin, when he expressed his criticism towards an international scene where the United States got to make decisions in a unilateral manner and used tough anti-Western rhetoric are all demonstrative examples. This propensity for disinformation reached its pinnacle in the Soviet era (Pacepa & Rychlak, 2013; Saberwal, 2018, p. 62).

Moreover, it should not be forgotten the fact that over the last 20 years, a defeated, demobilized and cracked "*red army*" has slowly, but surely, turned into an army of professionals, with state-of-the-art technology and with determination as Mother Russia's ambitions. From the objectives point of view, the Russian foreign policy of the last 100 years can be characterized by continuity. Many of the statements made by specialists in Russian territory more than 40-50 years ago are still valid today, and the new Russian Security Strategy took over the main force lines of the *Russian Foreign Policy Strategy from 2013*.

In a report conducted by the Strategic Studies Institute (SSI), part of the U.S. Army War College, the Russian strategy is defined by five elements: "(a) asymmetric warfare – the main base defining the

¹ Article available at <https://histoire.ens.fr/IMG/file/Coeure/David-Fox%20Potemkin%20villages.pdf>

Russian methods of conducting wars; (b) strategy of low intensity – a strategy that has been developed by Pentagon’s Joint Special Operations Command in 1980; (c) understanding and theoretical elaboration of the network-centric warfare; (d) definition of sixth generation warfare developed by general Vladimir Slipchenko; (e) strategic concept of reflexive control – which plays the role of maintaining the balance between the usage of military and non-military means in combat, in accordance with the strategic characteristics of each operation” (Deni, 2018, p. 19).

In the same context, in Putin’s era, Russia’s foreign policy is built around the following main goals, with applicability at both international and regional level: “(a) regain the status of great power and become one of the main actors on the international scene; (b) maintain its influence on post-Soviet countries and expand the sphere of influence of the ‘Russian World’ (Russkiy Mir) and Eurasian Union; (c) contain democracy and solidify a Russian style of governance” (Lough, Lutsevych, Pomerantsev, Secieru, & Shekhovtsov, 2014, p. 2).

Taking these two aspects into account, strategists and analysts concluded that Russia tends to use generation warfare in order to achieve its foreign policy objectives, and that this type of war follows eight different phases (Chekinov & Bogdanov, 2013), which could be seen in the conflict against Ukraine (Deni, 2018, pp. 19-20):

1. “develop non-military asymmetric warfare, which includes moral, ideological, information, diplomatic, psychological and even economic measures used in order to establish a favourable military, economic and political set-up;
2. conduct special operations, executed so as to mislead military and political leaders by coordinated measures carried out by using diplomatic channels, mass media and military and governmental agencies to present and promote false data and information;
3. use deception, intimidation and bribery of government officials and military officers to convince them to abandon their service duties and betray their native country;

4. use propaganda in order to destabilize and increase the dissatisfaction and discontent of the population, boosted by the Russian militants who engaged in subversion;
5. develop no-fly zones over the country in order to be attacked and use both private military companies and armed opposition units;
6. conduct military operations, followed by large-scale subversive and reconnaissance operations (which includes special operation forces, espionage in the space, intelligence, radio, diplomatic and economic domains);
7. use a mix of electronic operations, targeted information operations and air force operations, and of high precision weapons;
8. crush of remaining points of resistance and surviving enemy units by using field military operations” (Deni, 2018, pp. 19-20).

Therefore, it is true to say that, assimilated to the second main foreign policy goal, as well as to the first phase of the so called Russian generation warfare, the Russian state declared to have as a foreign policy objective for the next decades to counter the U.S. and Western influence beyond its close sphere of “privileged interests” (Rumer, 2018, p. 5), as declared in the provisions of the Military Doctrine of the Russian Federation, adopted on December 26, 2014, with regards to the military risks and threats:

“build-up of the power potential of the North Atlantic Treaty Organization (NATO) and vesting NATO with global functions carried out in violation of the rules of international law, bringing the military infrastructure of NATO member countries near the borders of the Russian Federation, including by further expansion of the alliance” (The Military Doctrine of the Russian Federation, 2015).

The same document describes Russia’s perspective upon the new modern conflict, by saying that for the Russian state modern wars will be fought on all levels (land, sea, air, space and information space), with accent on the later, because Russians consider that information is a leverage that ensures victory no matter the type of war (Ermus &

Salum, 2017, p. 58). In addition to this, the Russian state has developed further concern with the Rose Revolution that took place in Georgia in 2003 and the 2004 Orange Revolution from Ukraine, the Russian political scene considering that the status of regional power of Russia has begun to pale by losing influence in the post-Soviet countries to the West. Therefore, fearing that possible regime changes in neighbouring countries may also lead to regime changes on the Russian territory, Russia started to promote the theory according to which the West and its main partner, the United States, used soft power instruments (in particular, social networks, organized youth groups, and foreign financed non-governmental organizations – NGOs) in order to expand their influence in the neighbouring areas of the Russian Federation, destabilizing and weakening its power (Meister, 2016, p. 3).

In this context, Russian political elite concluded that Russia needs to develop both instruments to fight against the perceived outside influence and tools of offensive countermeasures, aspects reflected in the later decisions of Vladimir Putin, the President of the Russian Federation who put into practice the following measures (Meister, 2016, p. 6):

- isolated the Russian forces available to foreign influence (that could become Western instruments in an attempt to start a revolution on Russian soil), by introducing in 2004 the first laws to step up control over NGOs;
- reduced the foreign ownership of Russian media investments shares to 20 percent by February 2017 through a law passed by the Duma;
- increased state control of television broadcasters (which is one of the main sources of information with a coverage of more than 90% of the population), creating a pseudo-reality for the Russian public opinion, picturing the outside world as a stage for crises, accidents and wars where Russia is the only actor able to provide stability.

Therefore, Russian society has adopted, during the last ten years of Vladimir Putin's presidency, both aggressive and expansionist political strategies, based on geopolitical, revanchist and imperialist

ambitions, developing military capabilities, as well as its propaganda machine (Sazonov & Müür, 2017, pp. 9-10).

The Kremlin's concern for developing its mass media instruments can be reflected by the decision of the Presidency to "launch **an informational TV channel called Russia Today (RT)**", in order to compete with other "influential international channels, such as CNN International and BBC World". Even if the main objective of this channel was, as declared by Mikhail Seslavinsky, head of the Russian Federal Agency for Print and Mass Media, "to create a positive image of Russia abroad", nowadays RT is used as the main soft power tool of Kremlin, broadcasting in English, Spanish, and Arabic (Institute of Modern Russia, 2012).

Another soft power instrument used by Russian Federation as a propaganda tool is the **newspaper published by the Government of Russia, Rossiyskaya Gazeta**, which received a support of 156 million dollars from the President in 2013. According to a report of the Federal Agency for Press and Mass Media² (коммуникациям, 2012), this newspaper is another instrument in Russia's information mechanism, whose role is to promote and strengthen the image of the state outside its borders. As a proof, starting with 2007, Rossiyskaya Gazeta has published supplements on a monthly basis in 21 foreign publications, action considered to be part of the Russian project "*Russia beyond the Headlines*" (RBTH) (Institute of Modern Russia, 2012).

At national level, the Kremlin targets to obtain the control over the largest mass media, by **managing directly several national TV channels** (such as VGTRK and Channel One), or by **using government-owned corporations like Gazprom-Media** which owns the national channel NTV **or government-friendly companies like the National Media Group** (controlled by Yury Kovalchuk, a friend of the Russian president) which owns the channel REN-TV. Interesting is the fact that "the same National Media Group also owns 25% of the shares of Channel One, Russia's main TV station, the other 75% being controlled

² A federal executive body responsible for providing government services and managing government property in the field of press, mass media and mass communications, including public computer networks used in electronic media as well as in printing and publishing. See more at <http://www.fapmc.ru/rospechat.html>

by the government". Virtually, all the newspapers that benefit from wide-distribution inside the borders of the Russian state – such as *Komsomolskaya Pravda*, *Argumenty i fakty*, and *Izvestiya* – are trying to achieve objectives in favour of Kremlin: they only disseminate information that presents Russian authorities in a favourable light and stop the spread of negative information, portraying a false reality (The Propaganda of the Putin Era. Part One: In Russia, 2012).

So, massive expansions took place in the last decades within Russian mass media, directed at foreign markets such as the television broadcaster RT and the radio station Voice of Russia (which merged with RIA Novosti and formed Sputnik). Sputnik, another propagandistic tool, has developed into a state-funded network of media platforms, producing radio, social media and news agency content in local languages in 34 countries. Even if the Russian foreign media aimed at first to provide the Russian perspective of world at an international level, in response to the Western perspective offered by CNN and BBC, nowadays Russian mass media's main role abroad is to promote conspiracy theories to defame the Occident so as to destabilize the masses and make them question the decisions of their own governments and think that they are being lied (Meister, 2016, p. 8).

In an article published by the Institute of Modern Russia, a public policy think-tank that strives to establish an intellectual framework for building a democratic Russia governed by rule of law³, have been presented other partners of Russia's ruling elite that play an active role in the propaganda process at national level, as follows (The Propaganda of the Putin Era. Part One: In Russia, 2012):

- cultural figures (e.g. „Stanislav Govorukhin – filmmaker well-known to Soviet-era viewers, that has led Vladimir Putin's election campaign; Nikita Mikhalkov – Oscar winner filmmaker who made several films extolling Russian authorities”);
- “top hierarchy of the Russian Orthodox Church” (e.g. Patriarch Kirill strongly criticized the citizens who attended the rallies protesting against fraud during the Duma election

³ See more at <https://imrussia.org/en/about-us>

and he endorsed Putin in the presidential elections; Archimandrite Tikhon Shevkunov, “rumored to be to be Putin’s confessor – who produced in 2008 the film *The Fall of Empire: Lesson of Byzantium*, which presents “Putin’s mission”, and accuses the “destructive Westernization”);

- “education bureaucracy, particularly in schools” (the way the government influence the education act is demonstrated by different actions, such as: the “rewriting of history textbooks; agitation among students and their parents; the organization of «patriotic» line-ups before classes; gifts with symbols of the «party of power» to students”).

The same principles also apply to the Russian foreign policy, the Russian Federation expanding its propaganda machine by promoting fake news and conspiracy theories through mass media channels outside its borders, especially in post-Soviet countries (considered to be “in the Russian sphere of influence”), as well as in the European Union and the United States (as shown by a report of the Alliance for Securing Democracy, a project conducted by the German Marshall Fund, “Russia has interfered in the political processes of at least 27 countries of Europe and North America since 2004 by using disinformation operations and cyber-attacks”) (Laurinavičius, 2018, p. 5).

However, the propaganda instruments used to promote a perfect image of the Russian state at international level include besides traditional and modern mass media channels, **cyber tools** as follows:

- trolls – is a user whose online activity is intended to disrupt the activity of an online community by posting messages aimed at artificially diverting the attention of contributors to irrelevant topics or provoking emotional reactions. The user often uses multiple accounts in order to increase the number of posted messages and to create the illusion of an active conversation;
- bots – also known as web robot/WWW robot, is a software application that automatically runs certain scripts on the Internet, performing tasks that are simple and structurally iterative. Even if bots can be used for positive purposes to improve the quality of Internet services, they can also be

used with malicious purposes, for identity theft or the launch of DoS attacks. They can also be used to collect shared information on email lists, manipulate comments and/or votes on web pages that allow users to provide feedback. Bots as an online propaganda tool are used (1) for widespread (re)distribution of messages already posted by real users, and (2) in the process of filtering commentaries on social platforms that allow user feedback (Bradshaw & Howard, 2018, p. 8);

- honey pots – defined as a computer system/applications/data that simulates the behaviour of a real system to appear to belong to a network, but is isolated and closely monitored. It is created as bait for cyber-attacks so as to allow detection, identification, rejection, or study of a cyber-attack. The term has been developed during the Cold War and was used to refer to an operative agent carrying out espionage through seduction means and/or compromising the target. Today, virtual honeypot accounts include a sex appeal component, but acts by designing a personality similar to the target, sharing with it political points of view, rare passions and hobbies, or issues related to personal history, family, traumas, and so on. Through direct messages or e-mail conversations, honeypot accounts engage the target in seemingly unrelated conversations with national security or political influence (Weisburd, Watts, & Berger, 2016).

One eloquent example of the Russian use of cyber instruments in their foreign policy is represented by the increased number of Russian-language messages about NATO created by bots, as shown in the result of the study conducted by NATO Strategic Communications Centre of Excellence⁴. Moreover, the study also states that in March 2018, Russian-language bot activity about NATO surged past 11 000 messages per month, fact that again confirms the hypothesis according to which

⁴ Based in Latvia, it is a Multinational, Cross-sector Organization which provides comprehensive analyses, advice and practical support to the Alliance and Allied Nations.

NATO and the United States are one of the main enemies perceived by the Russian Federation (Fredheim, 2018).

Other Russian propagandistic instruments that are being used outside its borders are the **so-called pseudo-NGOs**, such as the Rossotrudnichestvo (Federal Agency for the Commonwealth of Independent States, Compatriots Living Abroad and International Humanitarian Cooperation), an institution established in 2008 in order to promote the Russian culture and language in the ex-Soviet countries, that has extended nowadays its area of operation. As declared by the Russian state, the institution was constructed as a response to the worldwide activities conducted by the U.S. Agency for International Development and for its activity the federation receives 78 million dollars annually from the state budget (Lough, Lutsevych, Pomerantsev, Secrieru, & Shekhovtsov, 2014, p. 3). Other such institutions include the Foundation for Compatriots (established in 2009), the Gorchakov Foundation (in 2011) and the Russkiy Mir (Russian World) Foundation, conceived in 2007, which aims to protect and maintain the culture and language of the Russian-speakers diaspora⁵ (Meister, 2016, p. 8).

In addition to this, the Russian Federation has taken further steps **to increase its control upon the local and regional activity of native/national NGOs**, beginning with 2004, when the first laws to step up control over NGOs were introduced so as to impose strict restrictions on the activities of Western NGOs in Russia, as well as on the foreign funding of independent Russian organizations. As a consequence, NGOs that apparently do not correlate their objectives with Kremlin's direction are stigmatized as "foreign agents", their work being hindered by immense bureaucratic hurdles, fact that hampered the process of accessing funds independent of state-controlled sources. Therefore, by March 2016, 122 groups had been labelled as foreign agents, and 14 groups were shut down (Russia: Government vs. Rights Groups. The Battle Chronicle, 2018). In addition to this, a blacklist (the so-called "stop list") has been drawn up by the Federation Council to ban certain foreign organizations (with a focus on those located in the United States, including The Jamestown Foundation, The Open Society Institute, The International Republican Institute, The National

⁵ See more at Russkiy Mir Foundation, <http://ruskiymir.ru/en/>

Democratic Institute, Freedom House), from working in Russia (Felgenhauer, 2015).

Moreover, the Russian government also has **many other partners, “including a large number of GONGOs (government-organized non-governmental organizations)** that are cooperating with the Ministry of Foreign Affairs on the basis of presidential grants funding (\$70 million per annum combined). In accordance with the results of a research conducted by experts from the Royal Institute of International Affairs, Chatham House, such groups include human rights groups (e.g. Moscow Bureau of Human Rights), youth groups (e.g. Youth Sodruzhestvo, Russian Youth Association), conservative think tanks and pro-Kremlin experts (e.g. Centre for Social Conservative Policy, Izborskiy Club, Foundation for Research of Problems of Russian Influence Abroad Democracy), election observers (e.g. Commonwealth of Independent States-Election Monitoring Organization – CIS-EMO, Organization for Democracy and Rights of People), Eurasians integration groups e.g. (Internationalist Russia, Foundation for Support of Eurasian Integration, Eurasians-New Wave, Young Eurasia)” (Lough, Lutsevych, Pomerantsev, Secieru, & Shekhovtsov, 2014, pp. 3-4).

A key pillar of the Kremlin propaganda machine is represented by **the global PR-agencies contracted by the Russian Federation in order to construct and disseminate worldwide positive messages aimed to improve the general perceived image of the Russian state**. Therefore, beginning with 2006, Russia employed, through the Russian bank Evrofinance Mosnarbank, Ketchum, one of the leading PR-agencies in the world, “for consulting and communication services during the period of Russia’s G8 Presidency”. During the last years, several contracts were signed with the same agency, expanding its activities to present Russia as a country with a favourable investment climate, to help the Russian company to find suitable channels to “*communicate with the media*” or even to make lobby at Time Magazine “to select Putin as its *Person of the Year* in 2007”. Given the fact that Ketchum PR agency conducted its main activities in the U.S., Kremlin also employed another PR company, GPlus Europe (Ketchum’s sister-company), to cover the same issues in the European market (Institute of Modern Russia, 2012).

In order to achieve its foreign policy objectives, the Russian Federation included in its strategy **orthodox groups**, that are either “affiliated with the Moscow Patriarchate (Den’Kreshchenia Rusi), either private sector orthodox oligarchs like Konstantin Malofeev and Vladimir Yakunin (who chair the St Basil’s Foundation and St Andrew’s Foundation respectively)”. These groups’ activities include promoting Russian language, Eurasian integration (Christianity and conservative values being the core of Eurasian civilization) and demonization of the EU association agreements, “defending human rights of compatriots, promotion of, defending the Russian interpretation of history, and mobilizing people on to the streets for protests in order to undermine sovereignty and create/intensify tensions” (Lough, Lutsevych, Pomerantsev, Secrieru, & Shekhovtsov, 2014, p. 4).

Last but not least, Russia included **social media** on its propaganda machine, adopting increasingly sophisticated techniques, including, as mentioned above in the section regarding cyber tools, trolling on news sites, fake hashtag and Twitter campaigns, and the close coordination between social media operations and other media. The main event that determined Kremlin to invest in its social media tools was represented by the anti-government protests in 2011, their online coverage leading the Russian government to increase its efforts to control, monitor, and influence the Internet and social media (Freedom on the Net 2016 – Russia, 2016). Russia’s propaganda on social media is considered to serve multiple purposes, including inducing paralysis, strengthening groups that share the same perspective and purposes as Russia, and creating alternative media narratives that match Russia’s objectives (Giles, 2016, p. 37).

With regards to social media, there have been identified three different levels of attribution for the actors integrated in Russia’s propaganda apparatus, based on their degree of accessibility and on their ability to further disseminate information, as follows (Helmus, et al., 2018, p. 11):

- “white” outlets – also known as overtly attributed, include official Russian government agencies (Ministry of Foreign Affairs, Russian state-controlled, state-affiliated, and state-censored media and think tanks – RT, Sputnik, the All-Russia

State Television and Radio Broadcasting Company – VGTRK, Channel One, Russian Institute for Strategic Studies);

- “gray” outlets – characterized by uncertain attribution, including conspiracy websites, far-right or far-left websites, news aggregators, and data dump websites (Weisburd, Watts, & Berger, 2016);
- “black” outlets – covert attribution, are outlets that produce content on user-generated media, but also add fear-mongering commentary to and amplify content produced by others and supply exploitable content to data dump websites, conducting activities through a network of trolls, bots, honeypots, and hackers (described above) (Weisburd, Watts, & Berger, 2016).

To conclude, information operations (or, in Russia’s framing, information confrontation) is a major part of Russia’s foreign policy, that helps the Kremlin to achieve its objectives by using less military force and avoiding direct confrontation with states perceived as enemies. Moreover, social media, together with cyber instruments, are one important element of Russia’s state-led information activities, which allows the Russian Federation to conduct covert operations, difficult to be tracked back or demonstrated. A leading analyst on Russian information warfare, Timothy Thomas, wrote that there is “*a real cognitive war underway in the ether and media for the hearts and minds of its citizens at home and abroad.*” (Thomas, 2015, p. 12; Helmus, et al., 2018, p. 1)

Instead of conclusions

Motto: *“One will readily agree that any army which does not train to use all the weapons, all the means and methods of warfare that the enemy possesses, or may possess, is behaving in an unwise or even criminal manner. This applies to politics even more than it does to the art of war.”* (Lenin V. I., 1920, p. 96)

Hybrid wars have not appeared as a novelty, but they have characteristics that make them different from the other types of wars. For this specific kind of warfare, different forces that are being used

either mix and become one single force or are used in the same battle space. The mix of irregular and conventional force capabilities is a challenging process, but this process has been encountered during history (Mattis & Hoffman, 2005; Hoffman, 2007).

As far as the definition of the hybrid warfare is concerned, there is no widely accepted approach to this term, but there are certainly differences in the ways this concept is perceived by each actor. For instance, in Russia's perspective, the hybrid warfare collocation has been replaced by generational warfare, which represents a combination of conventional and irregular instruments, based on psychological and information operations. On the other side, the European community identified hybrid wars as indirect conflicts that are conducted by (especially but not limited to) non-state actors, which use traditional and unconventional tools such as military force combined with cyber-attacks, propaganda, disinformation or terrorist attacks. Therefore, it is clear that there is a difference in Russian and Western terminology, which shows the actors' perspectives and certain aspects of the conflict (Dov Bachmann & Gunneriusson, 2015, p. 199).

However, the apparition and expansion of the hybrid warfare does not impact in a negative way the development of traditional or conventional types of war, but it has complicated the defence planning in the present times (Hoffman, 2009, p. 38). As John Arquilla, from the Naval Postgraduate School, has noted, "*While history provides some useful examples to stimulate strategic thought about such problems, coping with networks that can fight in so many different ways—sparking myriad, hybrid forms of conflict – is going to require some innovative thinking*" (Arquilla, 2007, p. 369). In the same context, "analysts highlighted the blurring lines between modes of war, by suggesting that one of the greatest challenges that will appear in the future will be created by states that opt for multiple tactics and technologies and blend them in innovative ways to meet their own strategic culture, geography and aims" (Hoffman, 2009, p. 35).

As far as Russia's foreign policy is concerned, this state identified the influence and activities of Western governmental and non-governmental institutions in the post-Soviet countries as instruments of war, whose perceived goal was to weaken the Russian government. In

this context, Moscow considered that is its right to react with the same methods to this non-linear warfare (that is, in its opinion, led by both NATO and the United States) and to respond with information operation and asymmetric means such as “little green men”, media manipulation, and exploitation of networks and NGOs (Meister, 2016, p. 5). The main foreign policy direction followed by the Russian state focuses on stopping the expansion of NATO’s and Western influence in the post-Soviet countries (which are considered to be in the Russia’s sphere of influence) and on creating a better picture of Russian culture and civilization outside its borders. Moscow’s strategy is to create facts on the ground to coerce its former partners turned rivals, to acknowledge Russia’s security interests and accept Russia’s importance as a great power to be reckoned with globally (Trenin, 2016).

As a proof, Russian strategic documents refer to a holistic concept of “information war”, which is used to fulfil two main objectives (Theohary, 2018, p. 9):

- to achieve political objectives without the use of military force;
- to construct a favourable international response to the deployment of its military forces, or military forces with which Moscow is allied.

Moreover, the new battle space, that encompasses political, economic, informational, technological, and ecological instruments, created by the Russian Federation in order to achieve its foreign policy aims is characterized by the following principles: influence is prioritized over destruction; inner decay over annihilation; and culture over weapons or technology (Fedyk, n.d.). On the same line, Russia appears to be using different mass media channels, especially social media tools, to spread a mix of propaganda, misinformation, and deliberately misleading or corrupted disinformation. Tactics also include data breaches of servers of U.S. political parties and other groups, releases and possible manipulation of sensitive documents in an attempt to influence the U.S. presidential election, and the manipulation of publicly available information on Russian activities in Ukraine (Theohary, 2018, p. 9).

Therefore, in order to adapt to the new forms of war that rose in the last decades, the Russian state has constructed and developed a set of unconventional, asymmetric, irregular tools which allow it to conduct new forms of conflict, without direct involvement. The main challenge for international actors in terms of establishing and ensuring national security will be to create proper responses and develop efficient instruments so as to overcome and be able to fight against new types of war.

References:

1. Arquilla, J. (2007). The End of War As We Knew It. *Third World Quarterly* 28, 369-386.
2. Aspaturian, V. (1969). Soviet Foreign Policy at the Crossroads: Conflict and/or Collaboration? *International Organization*, 589-620.
3. Aspaturian, V. (1971). *Process and Power in Soviet Foreign Policy*. Boston, Massachusetts, United States: Little, Brown and Company .
4. Banasik, M. (2015). How to Understand the Hybrid War. *Securitologia*, 19-34.
5. Bond, M. S. (2007). *Hybrid War: A New Paradigm for Stability Operations in Failing States*. Pennsylvania: U.S. Army War College .
6. Bradshaw, S., & Howard, P. P. (2018, January 29). Why does Junk News Spread so Quickly across Social Media? Algorithms, Advertising, and Exposure in Public Life. Retrieved from <http://comprop.oii.ox.ac.uk/research/working-papers/why-does-junk-news-spread-so-quickly-across-social-media/>
7. Butterfield, J., & Levintova, E. "(2009). How history and attitude to it are formed: school textbooks on the newest national history." *The Russian Public Opinion Herald: Levada Centre*3, 103-114.
8. Chekinov, S. G., & Bogdanov, S. A. (2013). The Nature and Content of New-Generation War. *Military Thought*.
9. Clausewitz, C. (2013). *On War*. Retrieved from Project Gutenberg: <http://www.gutenberg.org/files/1946/1946-h/1946-h.htm>
10. David-Fox, M. (n.d.). The Myth of the Soviet Potemkin Village. *séminaire de l'Université Paris 1 Panthéon Sorbonne et de l'ENS La Russie aux XIXe et XXe siècles : politique intérieure et influences internationales*. Sorbonne.

11. Deni, J. R. (2018). *Current Russia Military Affairs. Assessing and Countering Russian Strategy, Operational Planning and Modernization*. Carlisle, USA: U.S. Army War College.
12. Dov Bachmann, S., & Gunneriusson, H. (2015). Russia's Hybrid Warfare in the East: The Integral Nature of the Information Sphere. *Georgetown Journal of International Affairs*, 198-211.
13. Engels, F. (1949). The Defeat of the Piedmontese. *Neue Rheinische Zeitung*.
14. Ermus, A., & Salum, K. (2017). *Russian Information Warfare Against the Ukrainian State and Defen*
15. *ce Forces: April–December 2014*. Estonia: Kaitseväe Ühendatud Õppeasutused.
16. Fedyk, N. (n.d.). *Russian "New Generation" Warfare: Theory, Practice, and Lessons for U.S. Strategists*. Retrieved from Small Wars Journal: https://smallwarsjournal.com/jrnl/art/russian-%E2%80%9Cnew-generation%E2%80%9D-warfare-theory-practice-and-lessons-for-us-strategists-0#_edn6
17. Felgenhauer, P. (2015, July 9). *Extended List of 'Undesirable' Foreign NGOs Compiled in Moscow*. Retrieved from The Jamestown Foundation: <https://jamestown.org/program/extended-list-of-undesirable-foreign-ngos-compiled-in-moscow/>
18. Fredheim, R. (2018). *Robotrolling*. Riga, Latvia: Nato Strategic Communications Centre of Excellence.
19. (2016). *Freedom on the Net 2016 - Russia*. Freedom House.
20. Gat, A. (2001). *A History of Military Thought: From the Enlightenment to the Cold War*. Oxford: Oxford University Press.
21. Giles, K. (2016). *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. London: Thw Royal Institute of International Affairs, Chatham House.
22. Glenn, R. W. (2009). Thoughts on "Hybrid" Conflict . *Small Wars Journal* .
23. Helmus, T. C., Bodine-Baron, E., Radin, A., Magnuson, M., Mendelsohn, J., Marcellino, W., . . . Winkelman, Z. (2018). *Russian Social Media Influence: Understanding Russian Propaganda in Easter Europe*. Santa Monica, California: RAND Corporation.
24. Hoffman, F. (2007). *Conflict in the 21st Century: The Rise of Hybrid Warfare*. Arlington, VA: Potomac Institute for Policy Studies.
25. Hoffman, F. (2014, July 28). *On Not-So-New Warfare: Political Warfare vs Hybrid Threats*. Retrieved from War on the Rocks: <https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/>

26. Hoffman, F. G. (2009). Hybrid Warfare and Challenges. *Joint Forces Quarterly*, 34-39.
27. Johnson, R. (2017). The Evolution of Hybrid Threats Through History. In Y. Özel, & E. Inaltekin, *Shifting Paradigm of War: Hibrid Warfare* (pp. 3-8). Istanbul: Turkish National Defense University.
28. Kanwal, G. (2018). The Changing Character and the Taxonomy of Conflict. In V. Deshpande, *Hybrid Warfare – The Changing Character of Conflict* (pp. 1-24). New Delhi: Pentagon Press.
29. Laurinavičius, M. (2018). *A Guide to the Russian Tool Box of Election Meddling: a Platform to Analyze the Long Term Comprehensive Kremlin Strategy of Malign Influence*. International Elections Study Center.
30. Lenin, V. (1965). "Lessons of the Moscow Uprising". In V. Lenin, *Lenin Collected Works* (pp. 171–178). Moscow: Progress Publishers.
31. Lenin, V. I. (1920). *Collected Works*. Moscow: Progress Publishers.
32. Lough, J., Lutsevych, O., Pomerantsev, P., Secieru, S., & Shekhovtsov, A. (2014). *Russian Influence Abroad: Non-State Actors and Propaganda*. London: Chatam House. The Royal Institute of International Affairs.
33. Mattis, J. N., & Hoffman, F. (2005). Future Warfare: The Rise of Hybrid Warfare. *U.S. Naval Institute Proceedings*, (pp. 30-32).
34. McCuen, J. J. (2008). Hybrid Wars. *Military Review*, 107–113.
35. Meister, S. (2016). *Isolation and Propaganda. The Roots and Instruments of Russia's Disinformation Campaign*. Washington, DC: Transatlantic Academy.
36. Nemeth, W. J. (2002). *Future war and Chechnya : a case for hybrid warfare*. Monterey, CA: Naval Postgraduate School.
37. Pacepa, I. M., & Rychlak, R. J. (2013). *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*. USA: WND Books.
38. Racz, A. (2015). *Russia's Hybrid War in Ukraine, Breaking the enemy's ability to resist*. Helsinki: Finish INSTITUTE of International Affairs.
39. Rumer, E. (2018). Russian Strategic Objectives: It's About the. *Current Russian Military Affairs* (pp. 1-5). Strategic Studies Institute.
40. *Russia: Government vs. Rights Groups. The Battle Chronicle*. (2018, June 18). Retrieved from Human Rights Watch: <https://www.hrw.org/russia-government-against-rights-groups-battle-chronicle>
41. Saberwal, A. (2018). Russia and Hybrid Warfare – Achieving Strategic Goals without Outright Military Force. In V. Deshpande, *Hybrid Warfare: The Changing Character of Conflict* (pp. 62-73). New Delhi: Pentagon Press.

42. Sazonov, V., & Mür, K. (2017). Introduction: Russian Hybrid and Information Warfare. *ENDC Occasional Papers*, 9 – 12 .
43. Snegovaya, M. (2018). *Reviving the Propaganda State. How the Kremlin hijacked history to survive*. Center for European Policy Analysis.
44. *The Military Doctrine of the Russian Federation*. (2015, June 29). Retrieved from The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland: <https://rusemb.org.uk/press/2029>
45. *The Propaganda of the Putin Era. Part One: In Russia*. (2012, November 13). Retrieved from IMR – Institute of Modern Russia: <https://imrussia.org/en/politics/333-the-propaganda-of-the-putin-era>
46. *The Propaganda of the Putin Era. Part Two: The Kremlin's Tentacles*. (2012, December 5). Retrieved from IMR – Institute of Modern Russia: <https://imrussia.org/en/politics/344-the-propaganda-of-the-putin-era>
47. Theohary, C. A. (2018). *Information Warfare*. Washington D.C.: Congressional Research Service.
48. Trenin, D. (2016). *A Five-Year Outlook for Russian Foreign Policy: Demands, Drivers, and Influences*. Carnegie Endowment for International Peace.
49. Tulak, A. (2009). Hybrid Warfare and New Challenges in the Information Environment. *Joint Forces Quarterly*, 34-41.
50. Weisburd, A., Watts, C., & Berger, J. (2016, 11 6). Trolling for Trump: How Russia Is Trying to Destroy Our Democracy. *War on the Rocks*. Retrieved from <https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/>

REȚEAUA DE DEZINFORMARE „SPUTNIK” DE PE PLATFORMA TWITTER

Adrian BARBU*

Abstract

In an age where information means power, combat with weapons from the battlefields seems to have moved online. The main tools that actors use in the information battle are the same as those used hundreds of years ago - propaganda and disinformation, but the place in which they are promoted have been transformed due to technological developments. Now, the virtual environment and especially social media have become extremely attractive areas for those who want to promote fake messages in order to influence or mislead the opponent. Since 2011, with the anti-government protests in Russia, the Kremlin has invested heavily in the social media area, transforming it into an essential component of its information campaigns for the control, monitoring and influence of the virtual environment. Among the favorite targets of the actions subordinated to the information operations commanded from Moscow are the states in the immediate vicinity of the Russian colossus, respectively the states of Central Asia, the Caucasus, the Baltic states and Belarus, the Republic of Moldova and Ukraine, as well as the former communist states of Central Europe and of the East, including Romania. In the Romanian media, Sputnik Moldova-Romania is seen as the symbol of Russian propaganda. Not few were the cases in which journalists and Romanian experts proved how texts published on the news platform were created or cosmetized in order to mislead or generate favorable feelings for Moscow among readers. The Sputnik news agency, respectively its platform in Romanian, is one of the main promoters of Kremlin propaganda messages in the public space in Romania. This paper analyzes the way in which the most important representative of Russian propaganda in the local media acts in relation to Romanian online communities on the Twitter micro-blogging platform. In this regard, the activity of the Russian news agency's account has been assessed from a dual point of view: network analysis - how users coagulate around it and what are the characteristics of its ecosystem; content analysis - what are the main lines and messages diffused on the Twitter platform.

Keywords: *Disinformation, Propaganda, Russia, Twitter, Network, Sputnik.*

* PhD student Sociology and Social Assistance Faculty within University of Bucharest, email: adrian.barbu46@gmail.com

Introducere

Informația nu mai este doar un instrument de susținere a acțiunilor derulate prin intermediul altor mijloace, ci oferă noi oportunități de a derula activități non-letale ce pot afecta, înfrânge, descuraja sau exercita acțiuni de coerciție asupra adversarului.

Transformările produse în modul de desfășurare al conflictelor, în special pe fondul evoluției tehnologice, prin prisma mijloacelor și instrumentelor utilizate reprezintă o realitate ce nu poate fi neglijată. Manifestarea elementelor subsumate războiului hibrid sau celui informațional prin prisma unor evenimente de anvergură internațională, precum criza ucraineană declanșată în 2014, acuzațiile asupra influențării unor procese electorale și războiul civil sirian, de toate acestea fiind suspectate agenții guvernamentale de la Moscova.

Cele mai multe dintre presupusele acțiuni de propagandă derulate în secolul XXI, fie că vorbim de Federația Rusă, fie că ne raportăm la organizații teroriste sau extremiste, sunt asociate și au avut ca principal mijloc de propagare platformele de socializare. Social media a devenit un hub central în ceea ce privește derularea de acțiuni de propagandă și dezinformare. Tehnologiile din sfera social media permit crearea de conținut de către utilizator, colaborarea online sau partajarea de informații, fapt ce a permis transformarea sa într-un mediu propice pentru promovarea de mesaje menite să contureze, influențeze sau să inducă în eroare percepția, sentimentele și emoțiile sau procesele cognitive ale unor segmente de populație.

Războiul din Kosovo, conflictul dintre Hezbollah și Israel, „Primăvara Arabă”, criza din Ucraina și conflictele perpetue din Orientul Mijlociu, reprezintă doar câteva exemple, care au demonstrat puterea platformelor de socializare, în ceea ce privește capacitatea de a modela opinia publică, de a mobiliza mase de oameni, de a coordona activități militare sau de a colecta informații punctuale.

Lucrarea de față își propune să analizeze maniera în care cel mai important reprezentant al propagandei ruse din spațiul media autohton, agenția de știri rusă Sputnik (platforma în limba română), acționează în raport cu comunitățile de utilizatori din România existente pe platforma de micro-blogging Twitter. În acest sens, activitatea contului agenției de știri ruse va fi evaluat dintr-o dublă

perspectivă: analiză de rețea – din perspectiva modului în care coagulează utilizatorii în jurul său și care sunt specificitățile ecosistemului său; analiză de conținut – din perspectiva evaluării principalelor linii și mesaje propagate pe platforma Twitter.

Mașinăria de propagandă a Kremlinului

În octombrie 2018, Twitter a făcut public un set de date care conține peste 10 milioane de postări (*tweet-uri*), provenite de la 3.841 de conturi ce au conexiuni cu Agenția de Cercetare în Internet a Federației Ruse (IRA) și alte 700 de conturi conexe cu Iranul. Postările datează încă din anul 2009, conturile fiind identificate ca promotori de conținut fals în cadrul platformei, precum și de derularea de acțiuni de trolling, multe dintre ele, operate în preajma alegerilor prezidențiale din 2016 din SUA (Burgess, 2018).

Mai târziu, în luna ianuarie a anului 2019, pe platforma Facebook au fost suspendate 289 de pagini și 75 de conturi personale, care dețineau în total peste 790.000 de urmăritori (*followers*), acestea fiind identificate ca fiind pagini neautentice, care promovau mesaje false și care derulau acțiuni de trolling în cadrul platformei. S-a observat faptul că, majoritatea acestor pagini nu făceau altceva decât să reproducă conținutul livrat de agenția de știri rusă Sputnik. Acțiunile conturilor datau încă din august 2015, acestea investind în total aproximativ 135.000 de dolari, pentru propria promovare în cadrul platformei (Facebook, 2019).

Observăm, că Federația Rusă este implicată, în prezent, în campanii de propagandă și dezinformare în întreaga lume, așa-numita confruntare informațională fiind parte a politicii externe, dictată de la Kremlin. Moscova consideră că, se află într-o „confruntare cognitivă permanentă” atât în interiorul țării, cât și dincolo de granițe, iar acțiunile sale indică o abordare, care pare să acționeze după principiul „război informațional la scară largă” (Thomas, 2015, p. 12).

În această confruntare Rusia folosește propaganda, operațiunile în mediul virtual și entități de tip *proxy*, pentru a influența statele vecine, dar și pe cele din vestul continentului european. Acționează în această direcție, în special, prin intermediul televiziunii sale de stat, Russia Today (care transmite știri în engleză, arabă și spaniolă) și a

agenției de știri Sputnik care produce conținut pentru radio și mediul online în peste 30 de limbi (Helmus et al., 2015, p. 1).

Începând cu anul 2011, odată cu protestele antiguvernamentale din Rusia, Kremlinul a investit masiv în zona social media, transformând-o într-o componentă esențială a campaniilor sale informaționale, pentru controlul, monitorizarea și influențarea mediului virtual. De asemenea, a investit și în dezvoltarea așa-numitei „armate de troli”, care să le permită crearea de boți, ce pot fi configurați să acționeze automat pentru diverse scopuri (Giles, 2016, p. 30).

Printre țintele predilecte, ale acțiunilor subsumate operațiilor informaționale comandate de la Moscova, se numără statele din imediata vecinătate a colosului rus, respectiv statele din Asia Centrală, din Caucaz, statele baltice și Belarus, Republica Moldova și Ucraina, precum și fostele state comuniste din Europa Centrală și de Est, printre care și România (Helmus et al., 2015, p. 2).

Caracteristicile generale ale modelului contemporan al mașinării Kremlinului, care îi permite să fie atât de eficientă și capabilă, să influențeze indivizi, procese și fenomene sunt formate dintr-un set de 4 particularități (Paul, Matthews, 2016, pp. 2-9):

- are un volum mare și folosește canale multiple – sunt distribuite volume foarte mari de informații, care sunt diseminate prin intermediul unei game variate de canale; sunt folosite materiale în format text, foto, video, audio, promovate prin social media, televiziune, radio și presă scrisă (tipărită sau online);

Se bazează pe faptul că, o multitudine de surse sunt mai credibile și convingătoare decât una singură, în special, dacă prezintă argumente diferite care conduc la aceeași concluzie. De asemenea, oamenii tind să creadă că informația provenită din multiple surse are la bază perspective diferite, iar atenția auditoriului se îndreaptă astfel spre numărul de argumente și se pierde din vedere calitatea lor (Harkins, Petty, 1981, p. 628).

- este rapidă, continuă și repetitivă – informațiile sunt propagate cu rapiditate, entitățile promotoare ale mesajelor oferind o atenție sporită vitezei de reacție la evenimente, fără a se mai ține cont de realitatea obiectivă; deseori, o informație este

preluată în mod repetat pe diferite canale pentru a-i crește vizibilitatea, iar narativele care stau la baza lor sunt cosmetizate și relansate în spațiul public la intervale de timp;

Expunerea repetată a publicului la o anumită informație, perspectivă sau un argument, fie acestea și false, crește nivelul lor de credibilitate, ajungând să fie tratate, în cele din urmă, ca fiind adevărate (Lewandowsky et al., 2012, p. 113).

- nu prezintă angajament față de realitatea obiectivă – fie prin povești adevărate, în care sunt inserate informații false, fie prin fabricarea completă a unor narative; de asemenea, printre practicile mașinării ruse se mai numără citarea unor surse inexistente sau invocarea unor surse cu credibilitate, cărora li se atribuie în mod voit informații false;

Prin prisma volumului foarte mare de informații, la care este expus un individ în era în care trăim, diferențierea între o informație validă și un falsă este din ce în ce mai dificilă, în special, prin prisma lipsei de interes a cititorilor, care de cele mai multe ori, se mulțumesc să ia ca atare prima informația, cu care intră în contact, fără o evaluare prealabilă a sursei sau a validității conținutului informațional (Stuckemann, 2019, p. 20).

- nu prezintă consistență – mașinăria propagandistică nu diseminează aceleași teme și mesaje și nu face o problemă din a-și schimba radical poziționarea;

Contradicțiile pot crește nivelul de credibilitate, în momentul în care, un nou argument, o nouă idee este adusă în defavoarea alteia, prima dobândind un impact persuasiv mai mare. Când o sursă dă dovadă de faptul că prezintă o temă sau un subiect din perspective diferite, fie ele și contradictorii, există șanse considerabile pentru impulsivitatea încrederii cititorului în sursa respectivă, sub pretextul unui interes crescut pentru un anumit eveniment/fenomen (Reich, Tormala, 2013, p. 427).

În plus, ceea ce contribuie semnificativ la succesul acțiunilor de propagandă și dezinformare executate de Federația Rusă, este faptul că, poate să își adapteze narativele pe specificul socio-cultural al spațiului în care își dorește să acționeze. Spre exemplu, în ceea ce privește arealul est-european, discursul este personalizat în funcție de:

- atitudini, cultură și istorie (există state, precum România și Polonia cu un nivel relativ ridicat de rusofobie, dar și țări, precum Ungaria sau Bulgaria cu atitudini mai relaxate din acest punct de vedere);
- comunitatea rusofonă (state, precum Republica Moldova și statele baltice în care populația rusofonă este una semnificativă);
- cunoașterea limbii ruse (care facilitează transmiterea directă de mesaje);
- conexiuni ale liderilor politici de la Moscova cu cei din blocul est-european;
- raportarea populației la istoria URSS (Expert Forum, 2019).

Capacitatea și perseverența cu care Moscova implementează un model coerent și sistematic al acțiunilor de propagandă și dezinformare, au contribuit la transformarea modului în care conflictele sunt purtate în era informațională. Mașinăria dezvoltată de Federația Rusă, care operează la nivel global este prezentă și în spațiul virtual din România, cu modalități de acțiune personalizate și adaptate la spațiul autohton.

Propaganda rusă - ținta numită „România”

Sociologul Nicolae Țibrigan, explică faptul, că Rusia creează subiecte și tematici pentru fiecare țară în parte, concomitent cu „reciclarea” unor narațiuni la nivel regional, est-european, a doua categorie abordând subiecte mai generale, precum accentuarea poziției Federației Ruse ca putere globală, importanța unei scene internaționale multipolare, portretizarea unei lumi occidentale, care nu mai are valori morale și spirituale, fracturarea și ruperea Europei (Rusu, 2019).

În cazul României, propaganda pro-Kremlin, prin paleta de narațiuni rostogolite în spațiul mediatic, este diversă, de la cele anti-americane și anti-NATO, la cele care indică o conspirație a Vestului împotriva României (Rusu, 2019).

Un raport, din 2019, al Expert Forum arată faptul că discursul Kremlinului în România se axează în jurul a 4 direcții majore, respectiv:

- „Tema globală Soros - «statul paralel», valori culturale («problema LGBT»), imigrație”;
- „Stat de rangul doi, umilire națională, tratament dublu în UE”;

- „Costurile mari ale NATO și ale sistemului de securitate; riscurile prezenței militare SUA în regiune («poluare nucleară», risc militar)”;
- „Discursul anti-UE de tip post-colonial: acapararea piețelor, blocarea investițiilor, portul Constanța vs. Schengen”.

De asemenea, mai există o serie de alte narative conexe de România, pornind de la discursul anti-occidental, coroborat cu evidențierea unor elemente comune între mediul socio-economic cultural autohton și cel de la Moscova (Magdin, 2019). Spre exemplu, se aduce foarte des în discuție necesitatea revenirii la valorile tradiționale, creștin-ortodoxe, pe care România le împărtășește cu Federația Rusă. Se inserează deseori și elemente privind nostalgia față de perioadă comunistă și de realizările acelor vremuri. Nu în ultimul rând, mașinăria rusă de propagandă aduce pe tapet modelul economic capitalist pe care România l-a adoptat odată cu aderarea la UE și indică colapsul iminent al acestuia.

Unul dintre canalele prin intermediul cărui se rostogolesc mesaje dintre cele amintite anterior în spațiul mediatic din România este versiunea în limba română a site-ului agenției de știri ruse Sputnik International. Aceasta deservește publicul vorbitor de limbă română din Republica Moldova și România și este alimentată de o echipă redacțională de la Chișinău.

În zona mediatică din România, Sputnik Moldova-România este văzută drept simbolul propagandei ruse. Nu puține au fost cazurile în care jurnaliști și experți români au dovedit cum texte publicate pe platforma de știri au fost create sau cosmetizate cu scopul de a induce în eroare sau de a genera sentimente favorabile Moscovei în rândul cititorilor.

Metodologie

În vederea îndeplinirii obiectivului enunțat la începutul cercetării, cel de a evalua maniera în care cel mai important reprezentant al propagandei ruse, din spațiul media autohton (agenția de știri rusă Sputnik – platforma în limba română), acționează în raport cu comunitățile de utilizatori din România existente pe platforma de

micro-blogging Twitter, vor fi utilizate analiza de rețea și analiza conținutului știrilor distribuite, în cadrul platformei social media.

Astfel, a fost selectat ca interval de referință o perioadă de 2 luni, respectiv lunile septembrie și octombrie din anul 2019 și au fost extrase cele 1.878 de postări publicate de contul @sputnikmdro. Redistribuirea unei postări a fost luată în calcul drept unitate ce indică o conexiune între contul țintă și utilizatorul care a *share-uit* respectivul *tweet*. În continuare, au fost eliminați utilizatori care au redistribuit o singură dată un *tweet* al contului indicat, fiind luați în calcul, doar cei care au distribuit cel puțin două postări în intervalul analizat. A fost realizată această triere pe considerentul, că o unică distribuire nu relevă o adeziune sau preferință pentru conținutul publicat pe contul agenției de știri.

Ulterior, au fost extrase și suprapuse ego-rețelele utilizatorilor care îndeplinesc criteriile menționate pentru a obține imaginea rețelei. Datele au fost introduse în soft-ul Gephi și au fost rulate măsurători specifice pentru a detecta caracteristicile comunității virtuale delimitate.

În continuare, pentru a analiza conținutul știrilor distribuite, luând în calcul volumul informațional au fost eliminate din selecție postările care au obținut zero *retweet*-uri, adică 89% din total (1.685 din 1.878). Pentru a avea o abordare raportată și la *reach*-ul unei postări (audiența care intră în contact cu o postare) a fost calculată media redistribuirilor din totalul rămas, fiind obținut un scor de 1,52. Astfel, au fost menținute pentru demersul analitic cele care s-au situat peste media, adică *tweet*-urile cu minim 2 redistribuiri, respectiv 46 de materiale. Alături de conținutul știrilor au fost extrase și o serie de metadata asociate: data publicării, autorul, secțiunea în care a fost publicată, tag-urile (cuvintele-cheie).

În vederea elaborării analizei de conținut, a fost selectat articolul ca unitate de înregistrare, dat fiind faptul că, alegerea unei unități mai reduse ca dimensiune nu ar fi permis surprinderea corectă a existenței sau lipsei unei anumite teme în textele publicate. Astfel, au fost parcurse materialele pentru a identifica și observa care sunt temele prezente în eșantionul selectat. Pornind de la cele prezentate anterior privind retorica Kremlinului la adresa României, subiectele indicate au fost regrupate într-o grilă de trei teme majore, care a fost apoi

coroborată cu temele identificate în eșantionul de materiale selectat. Astfel, cele trei teme vizate sunt:

Temă	Mesaje urmărite
Subordonarea politico-economică față de puteri străine	Portretizarea, în special a NATO, UE și SUA, drept inamicii statului român, pe fondul imixtiunii acestora în viața politică și economică a țării (încălcarea suveranității naționale), fapt ce a transformat România într-o „colonie” a Occidentului, într-un stat de rangul doi în organizațiile din care face parte, motiv pentru care beneficiază de un tratament diferențiat, inechitabil față de alte state.
Reîntoarcerea la valorile tradiționale și glorificarea comunismului	Sublinierea unor elemente comune de ordin cultural, pe care România și Federația Rusă le împărtășesc, cu accent pe valorile creștin-ortodoxe și pe cele ale familiei tradiționale; prezentarea perioadei comuniste din România drept o perioadă prosperă, plină de realizări.
Manifestarea unor riscuri politico-militare	Evidențierea faptului, că prezența scutului anti-rachetă de la Deveselu reprezintă o amenințare la adresa securității României; prezentarea unor retorici agresive cu privire la dorința de obținere a autonomiei unor regiuni în care minorități etnice reprezintă populația majoritară.

Tabel nr. 1: Temele propagandei ruse în România (Sursa: autor)

Ecosistemul Sputnik Moldova-România și temele sale pe Twitter

În ceea ce privește structura rețelei de utilizatori care promovează *tweet*-urile contului @sputnikmdro, se constată, în primul rând, faptul că 20 dintre cei 31 de utilizatori (65%) de la care am pornit reconstrucția rețelei și care distribuie recurent postările contului menționat nu se regăsesc în lista de urmăritori (followers) ai Sputnik Moldova-România.

În urma parcurgerii pașilor de identificare a unei construcții a conexiunilor din jurul Sputnik, s-a constatat că avem de-a face cu o rețea formată din 147 de utilizatori și 836 de conexiuni, adică cu o structură fragmentată, cu un nivel al densității foarte scăzut (0.039).

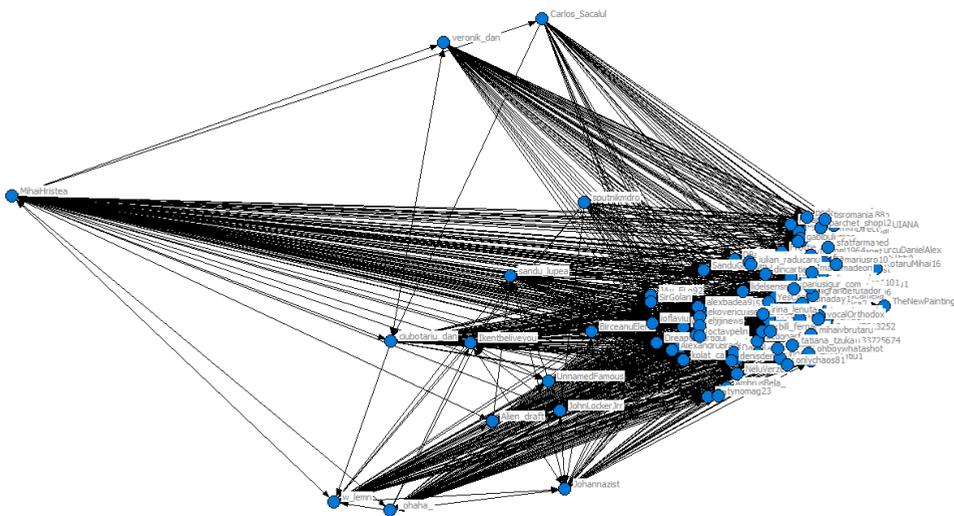


Figura 1: Rețeaua utilizatorilor de Twitter, care distribuie postările Sputnik România-Moldova (Sursa: autor)

Coeficientul de clusterizare se situează, de asemenea, la un nivel relativ scăzut (0,304), fapt ce indică o tendință slabă de coagulare/formare a subcomunităților la nivelul întregii rețele. Numai 4 dintre cei 147 de utilizatori fac parte din comunități dense cu tendințe puternice de clusterizare (coeficient de 0,750). În cazul

tuturor celor 4 actori, nodul cu cele mai multe conexiuni în rețea se află în vecinătatea lor.

Aplicând metodă hibridă de identificare a relațiilor reciproce¹, observăm că atât diadele cu conexiuni reciproce, cât și arcele reciproce, se situează la un nivel foarte scăzut, valorile fiind de 0,026, respectiv 0,050, fapt ce ne indică o posibilă structură ierarhică a rețelei. Astfel, aplicând măsurători care să arate nivelul de ierarhizare², am constatat că structura rețelei este una puternic bazată pe relații de subordonare (*hierarchy* = 0,9565). De asemenea, există puține conexiuni redundante, adică există un număr redus de lideri care controlează fluxul informațional în rețea, fapt ce indică un nivel ridicat al eficienței pe verticală (*efficiency* = 0,9368).

În urma evaluării conținutului articolelor selectate dintre cele distribuite pe platforma Twitter de către contul @sptunikmdro rezultă faptul că aproximativ un sfert (26%) din totalul materialelor analizate includ narative care se înscriu în linia discursului propagandistic promovat de Kremlin, respectiv conțin elemente subsumate celor 3 teme majore menționate. Se remarcă, ca pondere (13%), articolele care prezintă statul român ca fiind subordonat intereselor puterilor occidentale, în special prin prisma imixtiunii SUA în procesul politic din România. Cele privind manifestarea unor riscuri politico-militare reprezintă 8.7% din total, iar cele referitoare la reîntoarcerea la valorile tradiționale și glorificarea comunismului doar 4,3%.

Din cele 15 teme, identificate în selecția de articole, cea mai abordată a fost cea referitoare la „dispute politice interne” (17,4%), urmată de „subordonarea politico-economică față de puteri străine” (13%), „disfuncții în interiorul Uniunii Europene” (10,8%), „probleme sociale interne” (10,8%) și „manifestarea unor riscuri politico-militare” (8,7%). Remarcăm că, din perspectiva ponderii tematicilor abordate, în topul primelor 5 se regăsesc două dintre cele trei care sunt asociate cu retorica propagandei ruse, ambele având ca element generator factori de ordin extern, respectiv statele din Occident.

¹ O abordare care calculează relațiile reciproce, în raport cu numărul total de relații posibile (metoda diadelor), dar și în raport cu numărul total de relații existente (metoda arcelor).

² Krackhardt GTD.

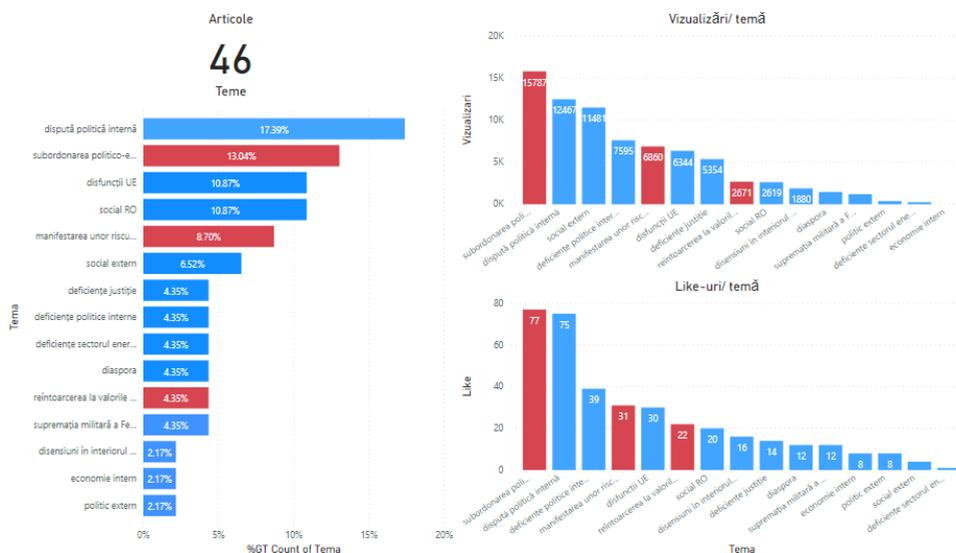


Figura 2: Analiza cantitativă a postărilor Sputnik România-Moldova de pe Twitter (Sursa: autor)

Din perspectiva posibilului impact asupra cititorilor, cifrele care indică numărul de vizualizări indică faptul că, în medie, cele mai vizualizate articole au fost cele subsumate temei subordonării politico-economice față de puteri străine, totalizând 20,7% din totalul vizualizărilor acumulate de materialele din selecție, fiind urmată de temele „dispută politică internă” (16,3%), „social extern” (15%), „deficiențe politice interne” (9,9%) și „manifestarea unor riscuri politico-militare” (9%). Raportat la numărul total de aprecieri (*like-uri*) obținute, topul se prezintă astfel: „subordonarea politico-economică față de puteri străine” (20,8%), „dispută politică internă” (20,3%), „deficiențe politice interne” (10,5%), „manifestarea unor riscuri politico-militare” (8,4%), „disfuncții în interiorul UE” (8,1%).

Dincolo de cele trei teme avute în vedere, se constată o apetență pentru publicarea unor articole despre sfera politică și socială internă și de la nivelul Uniunii Europene, cu accent pe „luptele” de pe scena politică internă și disfuncțiile construcției europene.

Concluzii

După o privire de ansamblu asupra structurii ecosistemului Sputnik Moldova-România de pe Twitter și a mesajelor articolelor publicate pe pagina web și distribuite pe platforma social media, putem extrage o serie de concluzii, cu privire la tiparul de acțiune pe unul dintre canalele utilizate de principalul promotor al propagandei și dezinformării din spațiul media autohton.

Tabloul în care se prezintă modul în care operează utilizatorul de Twitter @sputnikmdro se caracterizează astfel:

- Prezența într-o structură relațional fragmentată, dar puternic ierarhizată, în care nu există legături redundante, fapt ce înlesnește eficiența conexiunilor pe verticală în care un lider comandă, iar subordonații execută;
- Distribuirea preponderentă a materialelor din sfera politică, cu accent pe cele care privesc disputele politice interne și retoricile anti-occidentale, aspect ce confirmă faptul că mesajele Kremlinului pentru publicul din România țintesc subiecte referitoare la efectele negative pe care le are apartenența țării la NATO și UE (cel mai probabil din cauza faptului că mentalul colectiv din România este puternic caracterizat de rusofobie);

Astfel, putem conchide prin faptul că rețeaua de utilizatori din România de pe platforma Twitter, în cadrul căreia este prezentă agenția de știri Sputnik, are o arhitectură eterogenă și puternic ierarhizată, în interiorul căreia sunt vehiculate mesaje preponderent cu tematică politică, printre care se regăsesc principalele elemente de propagandă rusă promovate de-a lungul timpului în spațiul media din țara noastră, accesul fiind pus pe narativele subsumate temei „România – colonie a Occidentului”.

Referințe:

1. Burgess, M. (2018). *We finally know the full extent of Russia's Twitter trolling campaign*. Retrieved from <https://www.wired.co.uk/article/twitter-troll-data-russia-ira-iran/>
2. Facebook (2019). *Removing Coordinated Inauthentic Behavior from Russia*. Retrieved from <https://about.fb.com/news/2019/01/removing-cib-from-russia/>
3. Thomas, T. (2015). Russia's 21st Century Information War: Working to Undermine and Destabilize Populations. *Defence Strategic Communications, 1(1), 10-25*.
4. Helmus, T., Bodine-Baron, E., Radin, A., Magnuson, M., Mendelsohn, J., Marcellino, W., Bega, A., Winkelman, Z. (2018). *Russian Social Media Influence. Understanding Russian Propaganda in Eastern Europe*. Santa Monica, Rand Corporation.
5. Giles, K. (2016). *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. London, The Royal Institute of International Affairs.
6. Paul, C., Matthews, M. (2016). *The Russian "Firehouse of Falsehood" Propaganda Model – Why It Might Work and Options to Counter It*. Santa Monica, Rand Corporation.
7. Harkins, S. G., Petty, R. E. (1981). The Multiple Source Effect in Persuasion: The Effects of Distraction. *Personality and Social Psychology Bulletin, 7(4), 627-635*.
8. Lewandowsky, S., Ecker, U. K. H., Seifert, C. M., Schwarz, N., Cook, J. (2012). Misinformation and Its Correction: Continued Influence and Successful Debiasing. *Psychological Science in the Public Interest, 13(3), 106-131*.
9. Stuckemann, E. (2019). *Examining the Role of Source Credibility in the Vaccination Debate*. Jonkoping, Jonkoping University.
10. Reich, T., Tormala, Z. L. (2013). When Contradictions Foster Persuasion: An Attributional Perspective. *Journal of Experimental Social Psychology, 49(3), 426-439*.
11. Expert Forum (2019). *Raportul anuala EFOR 2019 – Renașterea populismului în Europa de Est*. Retrieved from <https://expertforum.ro/raport-anual-2019/>
12. Rusu, S. (2019). *Influența propagandei ruse în campania pentru alegerile europarlamentare din România. Interviu cu sociologul Nicolae Țibrigan*. Retrieved from <https://www.jurnalistii.ro/influenta-propagandei-ruse-in-campania-pentru-alegerile-europarlamentare-din-romania-interviu-cu-sociologul-nicolae-tibrigan/>
13. Magdin, R. (2019). *Disinformation and European Erosion in Romania*. Retrieved from <https://www.stopfake.org/en/disinformation-and-european-erosion-in-romania/>

**HISTORY AND MEMORY
IN INTELLIGENCE**

SOVIET RUSSIA AND THE “HYBRID WARFARE” AGAINST ROMANIA BETWEEN WW I AND WW II

Ioan Codruț LUCINESCU*

Abstract

World War I led to changes both on a European and a global level. Romania is a significant case/example considering the fact that in 1918, after the fall of the multinational empires, it achieved the goal of national unity. In the following years, the Romanian state promoted the peace established then, in order to strengthen its territorial integrity and alliances. The institutions of the national security system worked, since the end of the military actions, to fulfil this strategic objective.

Both the army and the national intelligence services were confronted with complex threats. “Great Romania” had, at the time, three neighbouring countries with an obvious revisionist foreign policy and territorial claims – Hungary, Bulgaria and Soviet Russia. By far the most dangerous enemy (both in terms of force and means) was the Soviet Union which never accepted the territorial losses of the Tsarist Empire and the loss of Bessarabia.

Lenin’s Russia and then Stalin’s Soviet Union attempted, in the two decades that separated WW I and WW II, to destabilize the Romanian state through means and methods that echo the modern “hybrid warfare” – from propaganda performed by the communist movement aimed at changing the constitutional order, to various attempts to ignite peasant revolutions (as a pretext for the Red Army intervention), and factory strikes, to an intensive espionage activity.

The paper aims to analyse on the one hand the ample subversive actions of the soviet secret services and, on the other, to look at the countermeasures that the Romanian intelligence structures adopted for their annihilation.

Keywords: *Romanian Army, the General Staff, First World War, Soviet Russia, Romanian intelligence services, interwar period, the Department for General State Security, hybrid warfare, Romanian Communist Party.*

* Senior Researcher PhD within “Mihai Viteazul” National Intelligence Academy, email: lucinescu.codrut@animv.eu

Introduction

In the European context generated after the end of World War I, Romania, as one of the dynamic actors of the international system created through the peace treaties of 1919-1923 had to face a double challenge, firstly, integrity (from an institutional, administrative and economic point of view), secondly, ensuring a state of security considering the fact that the eastern, western and southern borders were subjected to Soviet, Hungarian and Bulgarian revisionism.

Beyond the revolutionary propaganda which excited millions of people from the former Tsarist Empire, the communist leadership adopted an obvious repressive policy once it took over Russia. Denying the people's right to decide their own fate resulted in territorial loss, between 1917-1918, which was perceived by the new political-military elite as an act of "weakness" that had to be fixed as soon as possible.

The Romanian-Soviet relations were extremely tense in the following years, especially considering that the newly formed Soviet Union was considered to be, de facto, at war with the Romanian state (after breaking diplomatic relations in January of 1918), only waiting for an appropriate reason to engage in the real military offensive. In this matter, the words of Russian diplomat Maxim M. Litvinov, spoken to communist leader Cristian Racovski in 1920, are eloquent:

"We are now, formally, in a state of war with Romania. We consider that the Romanian troops occupy our territory and, formally, we can cross the Dniester without a declaration of war at any moment." (Constantiniu, 2010, p. 44)

But in order to achieve this strategic objective, a condition had to be respected – the significant weakening of Romania's capacity to react by internal destabilization, terror, assassinations, communist propaganda.

A difficult and extremely tense period follows for the national intelligence structures (firstly the military ones), said services had to, in the middle of the 3rd interwar decade, face an adversary (Russian secret services – VECHEKA, subsequently GPU and OGPU) capable and aggressive, even in the difficult conditions with which communist Russia was against while "applying" hits in the public opinion and not only; for example, the Senate attempt, December of 1920 (Troncotă,

2008, pp. 152-154) or the Tatarbunary uprising, September of 1924. Practically, an adversary that uses (excepting digital mass media propaganda, which didn't exist at the time) every instrument, method, and means presently known as being part of the “hybrid warfare” concept. Moreover, the study details them through the way Russia adapted them in agreement with the way events were carried out. We use the term “hybrid war” because Soviet Russia pursued the weakening of our state, and ultimately occupy a significant part of Romania (the re-occupation of Bessarabia was only one of the first steps) and not only weakening it in order to have certain advantages during negotiations on various topics.

Short introduction concerning the “hybrid warfare” concept

According to Joshua Ball, “hybrid warfare” is a notion referring to an extended area of hostile actions, where military force represents only a fraction and which are executed as part of a flexible strategy, with long-term objectives (Ball, 2019, p. 1).

Hybrid warfare is fundamentally an irregular, asymmetric war, which uses instruments like terrorist and guerrilla tactics, criminal actions, cyber operations, information attacks, put together perfectly so it is capable of affecting the security interests of the targeted state. The idea is affecting various domains/fields that are transformed into strategic ones, like the ones regarding informational operations made possible with support from favourable mass media. The objective is altering and transforming the will and support for engaging in the conflict of the targeted state, population or its leaders (Mattis & Hoffman, 2005).

In Russia’s case, according to the so-called “Gerasimov Doctrine” (2013) and other military theories (Monaghan, 2016), war and peace become notions whose borders keep getting more blurred as time goes on. “Methods of conflict” changed and they imply, nowadays, the massive appeal to political, economic, informational, and humanitarian and other non-military means. These can be supplemented, in particular cases, by using a part of the population (the same ethnic group with the aggressive state) as a true “5th column”, or by hidden armed forces.

Hybrid warfares are undeclared by the states, respectively, they are confrontations in which the military component isn't explicitly assumed and isn't, in any given case, singular. In hybrid warfare, not only the military weaknesses are essential, but so are the social ones, so non-military ones, for the one generating the aggression and tries to use them (ethnic tensions, weak and corrupted institutions, sensitive and highly emotional themes concerning that particular public, economical or energetical dependency etc.).

“Hybrid warfare” actions initiated by Soviet Russia against Romania at the beginning of the interwar period (1919-1925)

Based on historical reality and archived documents, we can appreciate the fact that the USSR engaged, between the two World Wars, in a veritable “hybrid war”, with variable intensities over two periods of time. Thereby, in the years 1919 – 1925, when Moscow thought that the “proletarian revolution” could take over Europe, it used considerable human and material resources to weaken capitalist societies and create proper conditions for a Red Army offensive on the continent.

The main target was the Balkan states – Bulgaria, Serbia (including its new provinces, especially Montenegro), Greece and Romania. Otherwise, our country was a strategic obstacle in the path of spreading communism in southern Europe. This is why it “benefited” from special treatment. That is why the Soviet Secret Services used procedures, means, and methods that could be considered as being part of the “hybrid warfare” arsenal, adapted to regional and historical conditions. Between 1919 and 1925, “hard” methods prevail in this complex conflict carried out by Soviet Russia against Romania:

- attempts to arrest the royal family and politico-military elite of the county (1918-1919);
- terrorist attacks with a major emotional impact on society: attacking the Senate (1920);
- massive infiltration of the worker's movement with propaganda agents to disrupt the country's economical life/well-being through strikes, sabotages etc.;

- setting up the Communist Party (May of 1921) to follow the Communist International policy (catchphrase “Romania imperial state that must be dismembered”);

- terrorist attacks in Bessarabia to affect the Romanian authorities credibility.

- maintaining a state of uncertainty in the Romanian society by massive infiltration of communist agitators in the country and the aggressive propaganda promoted by them Bessarabia is viewed by Moscow as being the base to launch “the worker's revolution” in Romania: Soviet secret services create a real “underground army” in the province, ammunition deposits, extended networks of informers etc.

The breakout of the Tatarbunary uprising (southern Bessarabia) in September of 1924 should have been the pretext of a Red Army intervention, to “free” the province and annex it to the newly formed Soviet Union; afterwards, depending on the evolution of those events, the Red Army would have moved forward deep into Romanian territory, towards the Balkan Peninsula, as evidenced by the numerous documents captured by the Romanian secret agents from communist agents infiltrated in the country.

The Tatarbunary uprising – the peak of the Russian “hybrid warfare” against Romania in interwar period

Based on the spread of the communist revolutionary movements in Europe, Soviet Russia started a strong offensive against our country fully using the “hybrid warfare” specific arsenal; this campaign which presumed to send hundreds and hundreds of secret agents of all categories on Romania's territory, as well as great amounts of currency, culminated in intensity in September of 1924. Then, in correlation with the ample communist campaign in Bulgaria and Serbia, triggering the final phase of the hybrid war (armed action to create the pretext of reinforcing the Red Army in Romania) was wanted.

In the middle of August 1924, the secret services informed the army's leadership of Moscow's plan to trigger in the following period a revolution on Romanian territory, through the Balkan wing of the Comintern. The communists' plan of action in Romania in September 1924 (known as the “Koralov Plan”) was approved in an important

meeting of the Russian and Balkan communist leaders under the supervision of Comintern's general secretary, Vasil Kolarov, and it stipulated the initiation of social movements (they were supposed to start between 10-15 September) in several regions of the country (5 of them), accompanying with triggering a campaign of terrorist attacks, assassinations and strikes, backed-up by armed gangs that arrived from Soviet territory (National Archives of Romania, Collection Police General Directorate, File no. 11/1924, f. 1-3).

Interesting to note is that the plan was supposed to be put in practice, initially, without any official involvement from the Soviet Union, another characteristic detail of hybrid war type operations. Hostile actions of the Romanian state only manifested in southern Bessarabia, in the Tatarbunary region, because there were certain factors that enabled such actions, the most important being the support received by the Soviet agents from the Slavs (Russian and Ukrainian) – representing the majority. In this way, with human and financial resources provided by the Communist International, true regional networks of espionage and terrorism, weapons and ammunition deposits, hiding places etc. were set up.

Taking into consideration the premises, on September the 15th 1924 the Communist Revolutionary Committee led by Andrei Kliușnikov (nickname Nenin), Soviet political commissar, decided to initiate the armed action. On the night of 15th/16th September, the communist agents took over the entire village of Tatarbunary, isolating it by cutting phone wires and shooting local riot cops. Nenin has communicated to the population that it's an undergoing revolution, Bessarabia self-proclaimed as "Moldavian Soviet Republic", and the Red Army entered its territory in order to drive away the Romanian army. Furthermore, he asked the men to arm themselves with the weapons found in secret deposits and fight against the Romanian troops (Moraru, 2008, pp. 229-232). To show their support of the rebellion, on 15th, 16th, and 17th September, the Soviet artillery stationed on the left shore of the Dniester River carried out military shooting manoeuvres, without launching projectiles on Romanian soil: Soviet Russia didn't want to start the war unless the certainty that Romania was unable to

respond in an efficient way existed – a method that can be easily placed under the philosophy of “hybrid warfare”.

Detachments of communist agents (20-30 people) take, in those days, the control over other villages and townships in southern Bessarabia, intimidating the population. The rebels created here revolutionary committees inspired by the soviet “style”, popular militia units and the Red Guards. The number of insurgents came to around 4.000-6.000, mostly of Ukrainian, Russian, Bulgarian ethnicity etc. The uprising wasn’t supported by the Romanian peasants/villagers and the Bessarabian Germans, which contributed to Russia’s failure.

In order to repress the communist activity, the Romanian Government sent artillery troops and a marine unit, the first clashes taking place on 16th September. On the morning of the 18th September, the Romanian troops launched an assault on Tatarbunary – the centre of the uprising, subjecting the place to an artillery attack. Unable to stand against the army, Nenin gave up the fight and ordered the retreat of the rebels, aiming to reach Soviet territory. But the Romanian units caught up, annihilating all of them. Andrei Kliușnikov, the main orchestrator of the fight, had the same fate – being killed on 19th September in the swamps near the Black Sea. On that same day, the main operations come to an end, the communist action being a disaster: hundreds of Soviet agents and their supporters in Bessarabia being killed or made prisoners (Moraru, 2008, pp. 233-234).

Even though it was fast and efficiently countered by the Romanian army (the communist rebellion only lasting for 4 days), the Tatarbunary action emphasized the great shortages of state institutions, firstly because of insufficient financial and human resources.

Rethinking the Russian policy towards Romania: using the “soft” methods of the “hybrid warfare”, 1925 - 1940

The categorical defeat suffered by the communists in the Balkans led to postponing the process of communizing Europe's south-eastern regions by two decades. Once the Soviet secret services' OGPU (the successor of CHEKA, see more about on Mitrokhin, 2008) actions were efficiently repressed, Moscow refined, in the next decade and a half (1925-1940), the methods and instruments used against our

country, said instruments being part of the hybrid warfare arsenal (the objective still being the one of partially occupying Romania):

- the massive use of secret services to break the informational side of our national security system (registered success in 1926) with the purpose of knowing, as precise as possible, our military capabilities;

- creates many “democratic” organizations, associations, “antifascist fronts” etc. that could act legally and spread communist ideas (in a hidden form) to the working class (the propaganda failed to be spread to the peasantry/rural population);

- reinforces the revisionist anti-Romanian propaganda on an international scale once the USSR was accepted in international organizations;

- creates the Moldavian Soviet Socialist Republic (October 1924) immediately after the Tatarbunary failure to maintain confusion in the population (the capital was at Tirasopol);

- it infiltrates both the left-wing parties (especially Romanian Social Democratic Party) and the far-right parties (Legionary Movement) with communist agitators to derail them from the inside;

- in Bessarabia, extended secret networks are formed in order to support a future attempt to occupy the province by the USSR – obvious success in June of 1940 when the withdrawal of Romanian army and administration was a disaster, resulting in the Soviets capturing the entire military inventory;

- it tries to undermine the country’s external alliances through pressure (and concessions) on some partners from the regional security formations (Yugoslavia, Czechoslovakia or Turkey).

Therefore, the means and methods varied and followed different kinds of actions, evolving and gaining amplitude with the help of the internal communist movement which, although was illegal, succeeded to create its own structures in the country. The direct link between the communists and the Soviet secret services and their hybrid warfare type actions are emphasized in the Romanian intelligence structures’ files, where it is specified that: “Members of the Romanian communist movement should not be seen as sons of the Romanian nation, followers of an ordinary political current, but as elements of the enemy

army, working with criminal means and purpose on the country's territory" (Troncotă, 2008, p. 121).

In this way, acting illegally, communist members and sympathizers created, especially in the industrial regions of the country, real networks meant to gather information for Moscow, as well as centres of propaganda and rumour spreading to maintain an uncertain environment in the Romanian society.

Otherwise, in January of 1930, the political bureau of PCUS met to go over INO's external operations (INO was an espionage structure of the main Soviet secret service – OGPU), ordering the organization to gather every possible information from interest zones for the Soviet Union: UK, France and Germany (main western powers), USSR's western neighbours: Poland (main regional enemy), Romania, Finland, the Baltic states and Japan (the great Asian rival power) (Volodarski, 2015, p. 39).

Soviet espionage operations against the state's institutions are, as well, amplified, with the purpose of knowing, in detail, Romania's military capacities, representing a crucial aspect considering that the end goal was triggering military operations. The importance of these secret actions showed itself in June of 1940 when the Soviet commandment further planned to occupy Bessarabia and to dismantling the Romanian army dispatched in the province, starting with the exact knowledge of the Romanian military tactics and its equipment, including weapon categories.

We point out that ever since the middle of the 3rd decade, the Romanian-Soviet "secret war" began. Regarding this fact, a known Russian spy, Boris F. Lago-ozarov, arrested in 1925 at Cernauti by the agents of the Department for General State Security (intelligence structure from the Ministry of Interior), confessed in his memoirs, that at Doftana were already imprisoned about 30 persons accused of espionage in the favour of USSR (Moraru, 2008, p. 151) (in the entire country were hundreds of Romanian citizens and foreign people detained for working in favour of the Soviet Union).

Because the archives belonging to the national defence institutions were destroyed during the World War or "wiped clean" of any sensitive information after the communist regime came to power in

Romania in 1948, few aspects are known about the Soviet agents' infiltration in the intelligence structures in the 4th interwar decade.

Although, according to the testimonies of several information officers with high functions during the World War, as lieutenant colonel Traian Borcescu (head of the Counterinformation Department in the Special Intelligence Service) we find out that major Tulbure, member of the army's secret service on the anti-communist wing, turned out to be a Soviet agent, according to the documents discovered by Romanian authorities after taking over Odessa (October 1941) (Troncotă, 2004, p. 46); not only he had access to extremely sensitive information regarding espionage networks set up by the Secret Services on Soviet land, but he also managed to infiltrate other "collaborators" through whom he can reinforce his spot and give better information to Moscow.

Even if the Soviet secret services will succeed in other spectacular actions, the most known case being the so-called "Ludovic Mircescu" case (1926-1930) through which the Moscow headquarters find out, in detail, the (Romanian) army deployment plan, with its strategy, weaponry, tactics etc. in the interwar period, registering a great failure.

The efficient policies to counter the far-left danger didn't allow the creation and consolidation, in the country, of a strong communist party to execute, like the parties in the Comintern, Moscow's orders. The resources given to the communist propaganda, diversion, terrorism, espionage actions (thousands of prepared men and millions of dollars – in gold – spent) didn't get communism "set up" in Romania until after 1945 and then only because the Red Army was occupying the country.

Conclusions

Lenin's Russia and then Stalin's USSR tried, in the two interwar decades, to destabilize the Romanian state through different means and methods – from internal propaganda with the help of the communist movement to attempt to spark a rural uprising and workers strike or intensive espionage activity on national territory.

With good reason, the American historian Keith Hitchins said that, for Romania, Soviet Union was “the hereditary enemy, always there, always being a threat to the existence of the country”.

The failure registered in 1924 once the Tatarbunary uprising (Romania) died down and the destruction of the strong communist movement in Bulgaria and Serbia makes Moscow rethink its mode of action (the idea of a military offensive isn't topical anymore), without giving up the strategic objective of taking over the southern part of the continent. For the failure of the plan were responsible, firstly, the national intelligence, military, and civilian structures. Even if it registered some successes in this “hybrid war”, the objective being weakening Romania, by reference to the human and material resources, we can say that Moscow suffered a visible failure. We state this because the re-occupation of Bessarabia by Soviet Russia in June 1940 was made possible due to the international situation in which the Romanian state was in as a consequence of France surrendering, the German-Soviet Non-Aggression Pact signed on August 23, 1939, and of the victorious German offensive in West.

It is proven through this historical step that the hybrid warfare has a very weak spot – it can't have the expected success while the targeted state has a strong society and politico-military elites that understand the danger and react in the proper way, even if initially the balance wasn't tipping in favour of the “victim”.

References:

1. National Archives of Romania, Collection *Police General Directorate*.
2. Ball, Joshua, (2019), “What Is Hybrid Warfare?”, in *Global Security Review*, June 10, <https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/>
3. Constantiniu, Laurențiu, (2010), *Uniunea Sovietică între obsesia securității și insecurității*, Editura Corint, București.
4. Mattis, N. James & Hoffman Frank, *Future Warfare: The Rise of Hybrid warfares*.
5. United States Naval Institute, November 2005, <http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf>

6. Mitrokhin Vasiliy, (2008), *"CHEKISM". Tales of the CHEKA, A KGB Anthology*, The Yurasov Press, London.
7. Monaghan, Andrew, (2016), *The 'War' in Russia's 'Hybrid Warfare'*, Strategic Studies Institute, https://ssi.armywarcollege.edu/pubs/parameters/issues/winter_2015-16/9_monaghan.pdf
8. Moraru, Pavel, (2008), *Serviciile secrete și Basarabia (1918 - 1991)*, Editura Militară, București.
9. Volodarski, Boris, (2015), *Cazul ORLOV. Dosare KGB*, Editura Litera, București.
10. Troncotă, Cristian, (2004), *Mihail Moruzov și frontul secret*, Editura ELION, București.
11. Troncotă, Cristian, (2008), *România și frontul secret 1859 - 1945*, Editura ELION, București.

**SECURITY PARADIGMS
IN THE 21ST CENTURY**

PRIORITIZAREA RISCURILOR ȘI AMENINȚĂRILOR LA ADRESA SECURITĂȚII NAȚIONALE A ROMÂNIEI. O PERSPECTIVĂ TRANSVERSALĂ 2013-2020

Cristian BARNA*
Valentin NICULA*

Abstract

Various approaches on the concept of security and the rise of numerous schools of thought within the security policies direct us towards a complex interpretation of the concept of security. The decisions, the policies and the strategies are greatly influenced by the paradigm in which we stand. The effectiveness of the interpretative horizon depends largely on innovation, complexity of analysis and the interdisciplinary in the security studies.

A mature approach to the issues of national security, based on advisory relationships and permanent feedback from the academic level, and civil society to the top of the political pyramid, will eliminate some of the frustrations and false perceptions of the Romanian society on security institutions.

In the current study we propose a transversal analysis on risk and threats to national security, having as starting point the outranking method investigation conducted in 2013 and the results of the Delphi technique investigation carried out in 2020.

Keywords: *concept of security, transversal analysis, security risk and threats, Delphi technique investigation.*

Introducere

Mediul internațional de securitate se schimbă rapid, iar proliferarea de noi riscuri accentuează starea de insecuritate a

* Associate Professor within “Mihai Viteazul” National Intelligence Academy, barna.cristian@animv.eu.

* Researcher PhD within “Mihai Viteazul” National Intelligence Academy, nicula.valentin@animv.eu.

sistemului global, motiv pentru care, în următorii ani, ordinea mondială va arăta semnificativ diferit, deoarece dinamica relațiilor internaționale indică aspirația spre un nou echilibru al balanței de putere. Toate acestea reprezintă variabilele unor scenarii prospective generatoare de strategii de securitate care ne marchează prezentul și ne vor influența viitorul! Aceste realități geostrategice ale mileniului al III-lea nu trebuie ignorate, deoarece se află pe acel “to do list” ale strategilor, într-o lume în care aceștia sunt constrânși, în analizele lor, de nevoia de prioritizare a resurselor în luarea unor decizii!

Nici România nu trebuie să aibă o altă abordare în acest sens! Prioritizarea riscurilor și amenințărilor la adresa securității naționale a României oferă factorilor de decizie posibilitatea cartografierii și cuantificării acestora în elaborarea strategiilor de securitate. Un astfel de demers poate oferi și un substrat analitic factorilor de decizie, din structurile de ordine publică, apărare și securitate națională pentru a se racorda, mult mai flexibil și eficient, la misiunile trasate de decidenții politici și pentru a asigura adaptabilitatea și interoperabilitatea categoriilor de forțe implicate în prevenirea și contracarea acestor riscuri și amenințări.

Prioritizarea riscurilor și amenințărilor la adresa securității naționale a României. Starea de fapt în 2013

La nivelul anului 2013, mediul de securitate era caracterizat de următoarele tendințe majore: accelerarea globalizării și integrării regionale, coroborate cu persistența acțiunilor care vizau: fragmentarea statelor; convergența rezonabilă a eforturilor depuse pentru structurarea unei noi arhitecturi de securitate, stabilă și previzibilă, în contextul unor tendințe anarhice crescute în unele regiuni, eforturi reînnoite ale statelor de a-și păstra influența pe scena relațiilor internaționale, dublată de creșterea cota de implicare a actorilor nestatali în evoluția acestor relații.

Având drept reper acest context geopolitic, în anul 2013 am considerat utilă și necesară derularea unei cercetări care să ofere o imagine cu privire la modul în care studenții angrenați în programele universitare de master în domeniul securității naționale și analizei informațiilor, potențiali factori de decizie, analiști sau formatori de

opinie în domeniu, prioritizează riscurile și amenințările la adresa securității naționale a României¹.

Într-o primă fază a cercetării, am efectuat o analiză de conținut asupra a două dintre cele mai importante documente strategice privind securitatea națională și apărarea în România: „Strategia de Securitate Națională a României. România Europeană, România Euro-Atlantică: pentru o viață mai bună într-o țară democratică, mai sigură și prosperă” (2007)² și „Strategia Națională de Apărare a României. Pentru o Românie care garantează securitatea și prosperitatea generațiilor viitoare”(2010)³.

În urma decelării acestor riscuri, amenințări, vulnerabilități și disfuncționalități la adresa securității naționale a României, așa cum sunt acestea menționate în documentele strategice supuse analizei, în următoarea fază a cercetării am aplicat tehnica analizei de conținut în vederea identificării modului în care acestea se regăsesc prezentate, în mod particular, în analizele unor experți în studii de securitate, apărare și intelligence din România, precum și a modului în care acesta sunt reflectate pe agenda publică sau în mass-media românești. În urma acestei analize a rezultat o listă de 99 indicatori, al 100-lea fiind lăsat la latitudinea respondenților pentru a fi decelat, în cazul în aceștia ar identifica și alte riscuri, amenințări, vulnerabilități sau disfuncționalități la adresa securității naționale a României.

Ulterior întocmirii listei indicatorilor, a fost elaborat un chestionar de răspuns raportat la care, celor 241 de respondenți, selectați din rândul studenților la programele universitare de master din București, care au ca obiectiv declarat promovarea culturii de

¹ Cercetarea derulată la nivelul anului 2013 a fost prezentată în cadrul Conferinței internaționale *Intelligence in the Knowledge Society*, ediția 2013 și a fost publicată în volumul *Proceedings of the XIXth international conference Intelligence in the Knowledge Society 2013*, ISSN 2392-7542, Editura Academiei Naționale de informații „Mihai Viteazul”, București, 2014; Articolul *Identifying risks and threats to Romania's national security. A sociological approach*, Cristian Barna, Valentin Nicula, pp. 271-290.

² *** *Strategia de Securitate Națională a României. România Europeană, România Euro-Atlantică: pentru o viață mai bună într-o țară democratică, mai sigură și prosperă*, 2007, www.presidency.ro

³ *** *Strategia Națională de Apărare a României. Pentru o Românie care garantează securitatea și prosperitatea generațiilor viitoare*, 2010, www.presidency.ro

securitate în cadrul societății civile și formarea de specialiști în studii de securitate națională, apărare și analiza informațiilor, li s-a solicitat să alcătuiască un clasament al acestor indicatori, în ordinea descrescătoare a pericolului pe care aceștia consideră că l-ar fi generat, la adresa securității naționale a României, în anul 2013.

Întrucât niciodată nu este de ajuns, subsumat indicatorului I.100, respondenții au identificat următoarele riscuri și amenințări la adresa securității naționale,: reglări de conturi între grupări de crimă organizată sub formă de atentate teroriste, destructurarea unor sectoare de producție prin falimentarea companiilor de stat scoase la privatizare, managementul defectuos în companiile de stat, scoaterea capitalului autohton din țară prin firme de tip off-shore, privatizarea excesivă și lipsa controlului statului asupra elementelor importante din economia României, incapacitatea sistemului sanitar și a sistemului de asigurări de sănătate de a răspunde solicitărilor unei populații tot mai îmbătrânite și de a face față subfinanțării, raportat la un procent de colectare a contribuțiilor sociale în continuă reducere, achiziționarea celei mai mari părți a produselor care funcționează pe baza de software de la producători externi (ex. China), dependența de sateliți comerciali și militari aparținând altor state, existența unui decalaj din punct de vedere al cercetării (fapt care, va crea o dependență față de țări avansate tehnologic în domeniul IT, nanosisteme și microsisteme, fonică, robotică, sănătate), amenințări produse de apariția unor virusuri foarte grave, care pun sănătatea populației în pericol, atacuri intenționate asupra populației cu virusuri special create în laborator, proliferarea violenței domestice și lipsa unor strategii/legi pentru combaterea acestui fenomen, regionalizarea/autonomia prea mare în regiuni în care sunt majoritare anumite grupuri etnice, dezvoltarea multilaterală accentuată a Chinei, deprecierea monedei naționale, rata mică de absorbție a fondurilor europene, implicarea unor instituții internaționale (de tipul FMI) în gestionarea bugetului României, îmbătrânirea demografică ce ar putea genera un import de forță de muncă și astfel, creșterea numărului de cetățeni străini (ceea ce în final ar putea conduce la tensiuni sociale sau xenofobe) lipsa preocupării pentru crearea de noi locuri de muncă, accesul neautorizat la informații clasificate și folosirea acestora în interese personale/de grup etc.

Ulterior prioritizării acestor indicatori, respondenții au fost solicitați ca, pentru primele zece riscuri, amenințări, vulnerabilități sau disfuncționalități decelate, să argumenteze decizia lor, un demers similar fiind derulat predictiv și în vederea prioritizării primelor zece riscuri, amenințări, vulnerabilități sau disfuncționalități la adresa securității naționale a României în anul 2020.

Rațiunea alegerii anului 2020 pentru a formula proiecții și prognoze de evoluție a riscurilor, amenințărilor, vulnerabilităților sau disfuncționalităților la adresa securității naționale a României este dat de faptul că acești studenți reprezintă o valoroasă resursă umană, din care, într-un interval de șase-șapte ani de la finalizarea studiilor (adică anul 2020), s-ar putea identifica și desăvârși profesional specialiști în analiza problematicii de securitate națională a României, argument susținut de analiza distribuției respondenților, după criteriul vârstei, care ne indică faptul că 76,54% dintre aceștia erau din categoria 22-30 ani.

Dintre aceștia, un procent de 80,5 % se aflau în categoria de vârstă de 22-30 ani, adică acele persoane din cadrul structurilor de securitate națională, apărare și ordine publică din țara noastră care, în anul 2020, ar putea să fi atins pragul maturității profesionale.

Faptul că, repartitia pe domenii de activitate a respondenților este una echilibrată, 128 dintre aceștia derulându-și activitatea, așa cum am menționat anterior, în cadrul structurilor de securitate națională, apărare și ordine publică, ceilalți 113 provenind din mediul civil, ne ofereau garanții cu privire la existența unui echilibru între părerile specialiștilor în domeniu și a reprezentanților societății civile (acei exponenți ai societății civile care manifestă preocupare pentru promovarea culturii de securitate).

În faza analitică a cercetării derulate, datele colectate de la respondenți au fost supuse unei interpretări statistice, tabelele de valori alocate indicatorilor fiind rodul acestor calcule statistice, aceste date fiind folosite în elaborarea topului indicatorilor riscurilor și amenințărilor la adresa securității naționale a României. În prioritizarea riscurilor și amenințărilor am considerat că o limită de analiză de minim 5 nominalizări pentru fiecare indicator nu afectează rezultatele cercetării, întrucât reprezintă ca valoare doar 0,34 % (pentru anul 2013), respectiv 0,38 % (pentru anul 2020) din totalul nominalizărilor.

Analiza statistică a răspunsurilor oferite de respondenți a fost făcută în două etape: în prima etapă au fost întocmite ierarhizările indicatorilor pe nivele, de la locul 1 până la locul 10, atât pentru anul 2013 cât și pentru anul 2020, conform frecvenței alocării indicatorilor de către respondenți, pentru fiecare dintre aceste locuri, respectând limita minimă de 5 nominalizări.

O analiză cantitativă a frecvențelor ne indică însă o prezență multiplă a unor indicatori în cele două clasamente de mai sus, pe poziții și cu frecvențe diferite (un exemplu în acest sens fiind indicatorii I.83 și I.37, în cazul clasamentului final pe anul 2013, sau indicatorul I.24 în cazul clasamentului final pe anul 2020). Din acest motiv, într-o a doua etapă a prioritizării, a fost realizată o ponderare a frecvenței indicatorilor pe care respondenții i-au atribuit celor zece locuri din clasamentul final pe anul 2013, respectiv pe anul 2020, stabilindu-se astfel frecvențele indicatorilor pe una dintre cele 10 locuri ale clasamentelor, rezultând următoarea prioritizare a riscurilor și amenințărilor la adresa securității naționale, în funcție de aceste frecvențe ponderate:

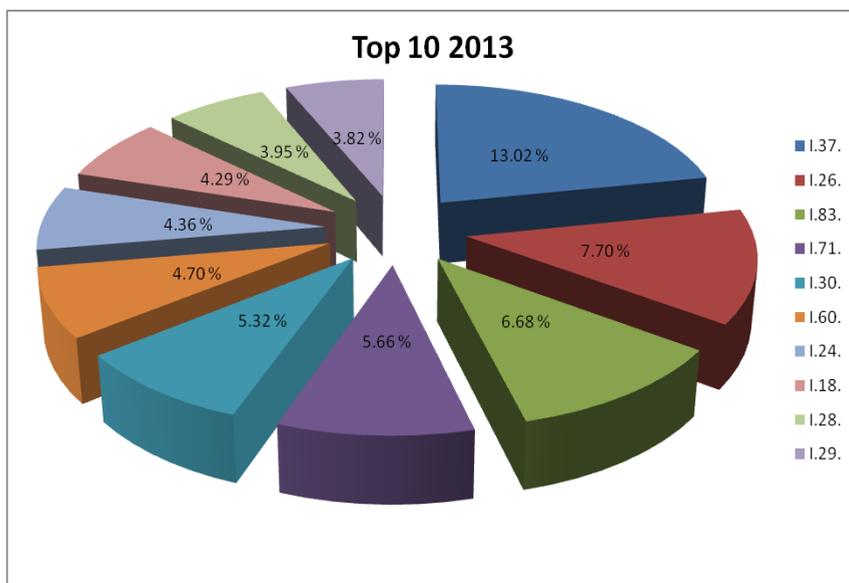


Figura 1: Clasamentului final al indicatorilor pe anul 2013
(Sursa: autorii)

Conform clasamentului frecvențelor ponderate pentru anul 2013, primele zece locuri sunt ocupate de următoarele riscuri, amenințări, vulnerabilități și disfuncționalități la adresa securității naționale:

- *I.37. corupția în rândul funcționarilor din administrația publică centrală și locală din România.*
- *I.26. creșterea nivelului de insecuritate socială și persistența stării de sărăcie la nivelul claselor sociale din România.*
- *I.83. migrația masivă a populației active, capabile de muncă și/sau înalt specializată (medici, asistente medicale, ingineri, profesori etc.).*
- *I.71. traficul cu ființe umane pe și/sau de pe teritoriul României care să alimenteze rețelele de prostituție sau cerșetorie;*
- *I.30. creșterea nivelului infracționalității la nivelul României.*
- *I.60. activitățile de spionaj ale serviciilor de informații din Federația Rusă, derulate pe teritoriul României.*
- *I.24. dependența accentuată de unele resurse (gaz, energie etc.), care nu se regăsesc într-o proporție suficientă pe teritoriul României.*
- *I.18. fenomene grave, de natură geofizică, meteoclimatică ori asociate (inundații, cutremure, alunecări de teren etc.).*
- *I.28. exercitarea iresponsabilă și ineficientă a puterii de către actorii politici din România, în dezacord cu principiile democrației și cerințele respectării drepturilor omului.*
- *I.29. comiterea unor atentate teroriste pe teritoriul României, de către elemente afiliate Al Qaeda, din cauza participării României cu trupe în teatrele de operații din Afganistan.*

Putem observa că, dintre primele zece poziții ale clasamentului, doar două se referă la riscuri și amenințări generate de actori externi, pe locul 6 fiind clasat riscul generat de activitățile de spionaj ale serviciilor de informații din Federația Rusă, derulate pe teritoriul României, iar pe locul 10, spectrul amenințării comiterii unor atentate teroriste pe teritoriul României de către elemente afiliate Al Qaeda, din cauza participării României cu trupe în teatrele de operații din Afganistan. Pe locul 7 al clasamentului se regăsește vulnerabilitatea generată de dependența accentuată de unele resurse (gaz, energie etc.),

care nu se regăsesc într-o proporție suficientă pe teritoriul României, o vulnerabilitate care poate să se transforme în amenințare la adresa securității naționale, în cazul unor acțiuni ostile ale Federației Ruse la adresa României, dependența de resurse manifestându-se mai ales față de gazele naturale, care sunt importate, într-un anumit procent, din acest stat.

Conform clasamentului, celelalte riscuri, amenințări, vulnerabilități sau disfuncționalități la adresa securității naționale a României sunt cele generate de acțiunile sau inacțiunile unor actori interni: corupția, exercitarea iresponsabilă și ineficientă a puterii, insecuritatea socială, sărăcia, migrația masivă a populației active, traficul cu ființe umane, infracționalitatea, fenomene grave, de natură geofizică, meteorologică ori asociate, acestea putând fi regăsite, în documentele strategice, ca riscuri și amenințări generate de guvernarea ineficientă, gestiunea ineficientă a treburilor publice sau proliferarea acțiunilor de criminalitate organizată, adică acele riscuri și amenințări ale căror apariție sau manifestare pot fi combătute prin implementarea unor politici și strategii publice eficiente.

În ceea ce privește clasamentul frecvențelor ponderate pentru anul 2020, putem observa, că ierarhizarea ponderată a frecvențelor cu minim cinci nominalizări, în ordine descrescătoare, ne oferă o imagine oarecum similară clasamentului din 2013, din primele zece poziții ale clasamentului doar vulnerabilitatea generată de dependența accentuată de unele resurse (gaz, energie etc.), care nu se regăsesc într-o proporție suficientă pe teritoriul României, clasată pe locul 1, fiind menționată de respondenți ca putând să amenințe securitatea națională a României din plan extern.

Celelalte riscuri, amenințări, vulnerabilități sau disfuncționalități la adresa securității naționale a României sunt tot cele generate de acțiunile sau inacțiunile unor actori interni, unele dintre ele, precum corupția, insecuritatea socială, sărăcia, migrația masivă a populației active, traficul cu ființe umane, infracționalitatea, fenomene grave, de natură geofizică, meteorologică ori asociate, perpetuându-se, în viziunea respondenților și în 2020.

Pe lângă acestea, între primele zece locuri ale clasamentelor au fost menționate, tot din categoria vulnerabilităților sau

disfuncționalităților care pot să se transforme sau să aibă un efect catalizator al unor riscuri și amenințări la adresa securității naționale: tendințele negative persistente în plan demografic (scăderea ratei natalității și creșterea ratei mortalității), degradarea mediului înconjurător, ca urmare a unor activități umane periculoase, dăunătoare sau iresponsabile (poluarea gravă, producerea unor pandemii etc.), precum și lipsa unor strategii eficiente de protejare a infrastructurilor critice (spitale, rețele de transport energie etc.).

De asemenea, lipsa unor strategii eficiente de protejare a infrastructurilor critice (spitale, rețele de transport energie etc.), care a intrat pe locul 10 în clasamentul pentru anul 2020, se afla pe locul 11 și în clasamentul pentru anul 2013, în vreme ce riscul la adresa securității naționale generat de activitățile de spionaj ale serviciilor de informații din Federația Rusă, derulate pe teritoriul României a „coborât” de pe locul 6 pe locul 11, indicator urmat tot de o amenințare provenită din partea unui actor extern, și anume Iranul, a cărui program nuclear militar ar putea deveni operațional până în 2020, respondenții considerând că există riscul ca acest arsenal să fie îndreptat împotriva statelor membre NATO.

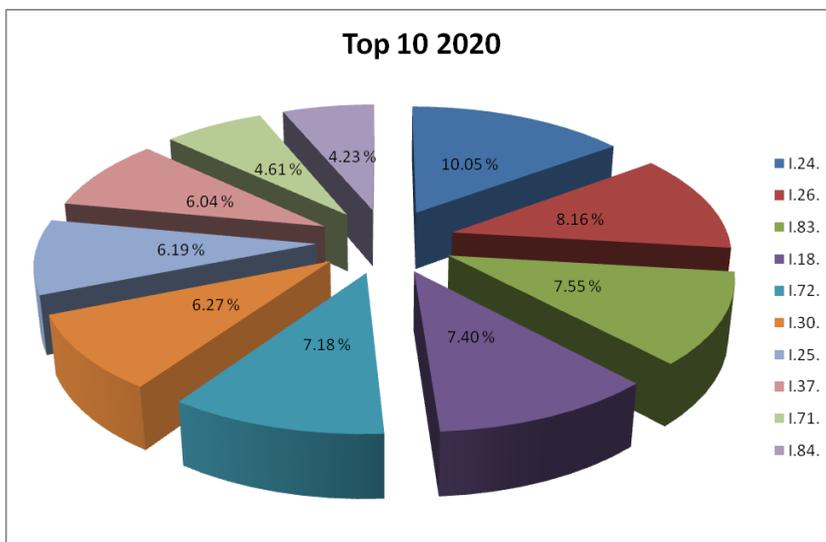


Figura 2: Clasamentul final al indicatorilor pe anul 2020
(Sursa: autorii)

- *I.24. dependența accentuată de unele resurse (gaz, energie etc.) care nu se regăsesc într-o proporție suficientă pe teritoriul României.*
- *I.26. creșterea nivelului de insecuritate socială și persistența stării de sărăcie la nivelul claselor sociale din România.*
- *I.83. migrația masivă a populației active, capabile de muncă și/sau înalt specializată (medici, asistente medicale, ingineri, profesori etc.).*
- *I.18. fenomene grave, de natură geofizică, meteoclimatică ori asociate (inundații, cutremure, alunecări de teren etc.).*
- *I.72. tendințele negative persistente în plan demografic (scăderea ratei natalității și creșterea ratei mortalității).*
- *I.30. creșterea nivelului infraționalității la nivelul României*
- *I.25. degradarea mediului înconjurător, ca urmare a unor activități umane periculoase, dăunătoare sau iresponsabile (poluarea gravă, producerea unor pandemii etc.).*
- *I.37. corupția în rândul funcționarilor din administrația publică centrală și locală din România.*
- *I.71. traficul cu ființe umane, pe și/sau de pe teritoriul României, care să alimenteze rețelele de prostituție sau cerșetorie.*
- *I.84. lipsa unor strategii eficiente de protejare a infrastructurilor critice (spitale, rețele de transport energie etc.).*

Momentul validării: 2020

Întrucât ne aflăm în anul 2020, adică momentul în care a ajuns la termen predicția respondenților chestionați în 2013, am considerat util să ne aplecăm din nou asupra acestor riscuri, amenințări, vulnerabilități și disfuncționalități la adresa securității naționale a României.

În această a doua fază a cercetării, derulată la șapte ani distanță, o variabilă care ar fi putut vicia cercetarea noastră este variabila timp și anume punerea în aplicare, de la momentul derulării primei faze a cercetării, a „Strategiei Naționale de Apărare a Țării pentru perioada 2015 – 2019. O Românie puternică în Europa și în lume”⁴, unde riscurile, amenințările, vulnerabilitățile și disfuncționalitățile la adresa

⁴ *** *Strategia Națională de Apărare a Țării pentru perioada 2015 - 2019. O Românie puternică în Europa și în lume*, www.presidency.ro

securității naționale a României sunt diferit prezentate. Astfel, în documentul strategic invocat nu mai apar disfuncționalitățile, ca și categorie distinctă, unele dintre acestea regăsindu-se însă, în categoria vulnerabilităților, iar unele riscuri, amenințări și vulnerabilități sunt menționate diferit.

În ceea ce ne privește, am făcut o analiză comparativă pentru a stabili dacă riscurile, amenințările și vulnerabilitățile, așa cum sunt menționate în „Strategia Națională de Apărare a Țării pentru perioada 2015 – 2019. O Românie puternică în Europa și în lume”, se regăsesc sau nu în lista indicatorilor, rezultând că lista indicatorilor le acoperă, în mod exhaustiv.

Întrucât în etapa aceasta a cercetării am dorit să închidem cercul analitic, privind riscurile, amenințările și vulnerabilitățile la adresa securității naționale a României, am decis să ne adresăm acelei categorii socio-profesionale care a sprijinit, în mod indirect, elaborarea listei indicatorilor în 2013.

Mai precis, întrucât în scopul elaborării listei indicatorilor supuși prioritizării am analizat modul în care, analiști militari, de politică externă și de securitate, cadre universitare și cercetători științifici cu expertiză în relații internaționale, studii de securitate și geopolitică, respectiv formatori de opinie din spațiul public se raportau la riscurile, amenințările, vulnerabilitățile și disfuncționalitățile din documentele strategice menționate, în anul 2020 am decis, folosind o variantă customizată a metodei Delphi, să ne adresăm acestor categorii socio-profesionale pentru a le solicita să prioritizeze indicatorii.

Pentru selecția experților, am făcut analiză a profilurilor acestora și am ales 10 dintre cei mai renumiți analiști militari, de politică externă și de securitate, respectiv cadre didactice din învățământul superior și cercetători științifici din domeniile relații internaționale, studii de securitate și geopolitică, respectând inclusiv criteriul dispersiei geografice (aceștia desfășurându-și activitatea în centre universitare din București, Cluj, Sibiu, Timișoara și Iași).

Experților selectați le-am adresat aceeași cerință, de a analiza lista indicatorilor, elaborată la nivelul anului 2013 (pentru a exista posibilitatea derulării unei analize comparative a rezultatelor obținute cu cele ale respondenților din 2013, care au formulat predicții pentru

2020, mai ales că lista este acoperitoare și în anul 2020, așa cum am arătat mai sus) și să întocmească același tip de „clasament”, în care pe locul 1 să poziționeze cel mai grav risc, amenințare sau vulnerabilitate, urmând apoi să le ierarhizeze pe următoarele 10, în ordinea descrescătoare a nivelului de amenințare. De asemenea, le-am solicitat și să motiveze (în 3-4 propoziții) de ce au optat pentru amplasarea indicatorului respectiv pe acel loc.

În faza analitică a cercetării derulate, datele colectate de la experți au fost supuse unei interpretări statistice, tabelele de valori alocate indicatorilor fiind rodul acestor calcule statistice, aceste date fiind folosite în elaborarea topului indicatorilor riscurilor și amenințărilor la adresa securității naționale a României.

Dacă ar fi să alcătuim un clasament al primelor zece riscuri și amenințări la adresa securității naționale, luând în considerare doar numărul de nominalizări, fără a corela cu poziția din clasament, acesta ar cuprinde, în ordine descrescătoare, doar 31 de indicatori se regăsesc în opțiunile exprimate de experți, conform următoarelor motivații furnizate pentru introducerea în lista celor 10 cele mai grave riscuri, amenințări sau vulnerabilități:

○ **I.100.** – 5 din 10 experți au simțit nevoia de a introduce **un indicator nou în clasament**, în majoritatea covârșitoare acești indicatori fiind corelați, cum era de anticipat, cu **manifestarea pandemiei COVID-19**:

- **îmbolnăviri COVID-19 din cadrul personalului medical** – lipsa investițiilor în echipamente medicale adecvate;
- **lipsa unor capacități de producție pentru fabricarea anumitor produse vitale în situații de criză** – în contextul pandemiei COVID-19, dependența de produse care nu se mai fabrică în România (vaccinuri, echipamente medicale etc);
- **impactul macro-financiar generat de pandemia COVID-19** – creșterea cheltuielilor și scăderea încasărilor statului român generate la bugetul de stat pot genera o explozie a datoriei publice, precum și dificultăți în asigurarea finanțarea securității naționale (de la angajamentele asumate ca stat membru NATO până la asigurarea ordinii publice) și a bunurilor și serviciilor de utilitate publică;

- **izolarea economică a României în contextul crizei generată de pandemia COVID-19** – poate avea consecințe asupra prosperității economice și asigurării ordinii publice;
 - **evoluția politică și economică la nivel internațional, determinată de pandemia COVID-19** – efect asupra prosperității economice a populației, precum și a politicii externe și de Securitate a României;
 - **accentuarea disoluției autorității statului, coroborată cu efectele sociale, economice și financiare generate de pandemia COVID-19** – disoluția autorității statului se poate accentua, ca urmare a lipsei de profesionalism la toate nivelele de conducere, a crizei de lideri cu profil profesional și moral la standarde înalte, a corupției, a scăderii încrederii populației în organele de stat;
 - **dependența de infrastructura economică a Republicii Populare Chineze** – China va urmări să condiționeze ajutorul medical în pandemia COVID-19, acordat statelor UE, inclusiv în relația cu România.
- *1.26. Creșterea nivelului de insecuritate socială și persistența stării de sărăcie la nivelul claselor sociale din România*

Migrația masivă a forței de muncă, tendințele demografice negative, lipsa reformelor în educație determină insecuritate socială și permite dezvoltarea unui teren fertil pentru mișcări politice și sociale care pot avea drept efect scăderea capacității statului român de exercitare a suveranității. Grupuri sociale marginalizate economic pot constitui o pepinieră în acest sens, fiind diluată semnificația conceptelor de patriotism, națiune, iubire de țară, suveranitate, integritate teritorială etc.

Încă din 2015, Academia Română atrăgea atenția asupra profilului de *stat neo-feudal* al țării noastre, fiind semnalată lipsa coeziunii politice în ceea ce privește măsurile economice posibil a fi implementate și derulate pe termen lung.

Ca urmare a iminentei crize economice, generate de pandemia COVID-19, populația va sărăci și mai mult, iar pierderea locurilor de muncă și imposibilitatea geografică de a

migra a cetățenilor români, în căutarea de locuri de muncă, va conduce la creșterea numărului de asistați sociali, care vor trăi la limita subzistenței.

○ *1.37. Corupția în rândul funcționarilor din administrația publică centrală și locală din România*

Lipsa digitalizării supraîncarcă efortul bugetar și aparatul administrativ al statului. Corupția din rândul funcționarilor conduce la relații de șantaj și complicitate, cu rolul de a obține avantaje și bunuri necuvenite, dar și de a bloca anumite proiecte. Aceste „caste” se pot transforma în grupuri de presiune informale care pot să blocheze inițiative ale statului român. Spre exemplu, corupția a condus la defrișări masive și tăieri ilegale de păduri, la folosirea defectuoasă a fondurilor de stat, fraudarea unor finanțări europene și a unor fonduri de dezvoltare locală, privilegierea unor actori economici și persoane fizice. Când corupția se combină cu lipsa de profesionalism, asistăm la un aparat administrativ a cărui infirmitate nu poate răspunde nici măcar nevoilor de bază ale cetățeanului, ca să nu amintim standardele de la nivelul UE, un garant pentru investitorii străini care, inevitabil, interacționează cu acest aparat administrativ.

Corupția contribuie și la scăderea încrederii cetățenilor în ordinea constituțională, continuând să fie un fenomen extins, ca urmare a lipsei de educație și de conștiință civică, a lipsei mecanismelor de control și verificare, a lacunelor legislative și a proceselor birocratice.

○ *1.49. Agresiuni informaționale (campanii mediatice denigratoare, campanii de dezinformare etc.) la adresa unor lideri politici, membrii ai administrației publice centrale sau locale, lideri militari etc., din partea unor actori interni (ONG-uri, partide politice, reprezentanți ai mass media etc.), din cauza aservirii acesora unor interese străine (ale Federației Ruse, Ungariei, Iranului, Ucrainei etc.)*

Agresiunilor informaționale creează realități alternative, afectează capacitatea de a discerne a oamenilor. În prezent, pentru exercitarea influenței politice, este mai facil să ocupi/controlezi spațiul informațional al unei comunități decât să cucerești un teritoriu. Acțiunile de propagandă, intoxicare

media, manipulare, dezinformare, informare parțială, operații de influență etc, au scopul de a zdruncina încrederea populației în instituțiile statului.

Agresiunilor informaționale conduc la slăbirea coeziunii sociale, determină scăderea încrederii în clasa politică și afectează coeziunea națională. Agresiunile informaționale ale Federației Ruse, mai ales asupra liderilor din domeniul securității naționale, expuși mediatic pe timpul pandemiei COVID-19, pot influența populația cu moralul scăzut, care se simte neajutorată.

Aceste agresiuni informaționale sunt potențate și de acoperirea mediatică cu privire la capacitatea operațională a Federației Ruse referitoare la: extinderea și modernizarea flotei Mării Negre, poziționarea unor capacități aeriene ofensive și de apărare antiaeriană în Peninsula Crimeea și în regiunile controlate din Georgia (strâmtoarele Bosfor și Dardanele intră în raza de acțiune, fapt ce ar putea îngreuna dislocarea, la nevoie, a flotei militare NATO în Marea Neagră).

○ *1.22. Lipsa de profesionalism a funcționarilor din administrația publică centrală și locală din România*

Ca urmare a implicării clasei politice în administrație, a promovării pe criterii subiective, a nepotismului și corupției, va continua deprofesionalizarea administrației publice centrale și locale.

Corupția, nepotismul și politizarea aparatului de stat pot conduce la scăderea încrederii cetățenilor în ordinea constituțională, precum și la o risipă de resurse generată de ineficiența unor politici publice

Lipsa de profesionalism, la fel ca și luarea unor decizii cu tentă politică doar pentru câștigarea de capital electoral ar trebui considerate amenințări la adresa securității naționale.

Funcționarii vor fi tot mai puțin capabili să elaboreze și să implementeze strategii, să îndeplinească cerințele din fișele posturilor, vor îngreuna fluxurile și procesele birocratice. Ca atare, optimizarea aparatului administrativ central și local este o prioritate imediată și trebuie făcută prin regândirea structurilor,

reducerea personalului, încadrarea și promovarea pe funcții doar pe criterii profesionale, fără implicarea clasei politice, sub nivelul de secretar de stat.

Factorii de decizie trebuie să beneficieze de expertiză în domeniu. Dar, constatăm că orice fel de decizie a ajuns să fie contestată și ca urmare a faptului că nu au fost identificate criteriile reale de nominalizare/numire a funcționarilor pe posturi.

Suntem în continuare tributari unor tare ale societății. Dintre toate „relele”, persistența unei norme de tipul „merge și așa!” în rândul aparatului de stat este atât păguboasă cât și profundă.

- *1.50. Agresiuni informatice din partea Federației Ruse asupra unor infrastructuri critice (rețele hidrografice, sectorul energetic, sectorul militar, administrativ etc.) ale României, din cauza permitterii forțelor navale ale SUA să folosească facilitățile navale din portul Constanța sau facilitățile aeriene de la baza Mihail Kogălniceanu din județul Constanța*

Federația Rusă dispune de capacitatea logistică necesară derulării unor astfel de operațiuni, fiind manifeste inițiative de obținere a unui avantaj tehnic/tehnologic într-un mediu/spațiu nereglementat la nivel internațional.

Modelul de acțiune cibernetică Estonia 2007-2008 poate fi replicat oricând și oriunde: acțiuni specifice confruntărilor asimetrice generate de interesele divergente ale SUA și Federației Ruse pot fi folosite ca mijloc de coerciție împotriva țării noastre, dată fiind poziționarea geostrategică a României.

- *1.60. Activitățile de spionaj ale serviciilor de informații din Federația Rusă, derulate pe teritoriul României*

Este binecunoscut efortul serviciilor de informații rusești de a derula operațiuni de spionaj oriunde pe glob. Federația Rusă folosește o gamă largă de metode și tehnici specifice intelligence-ului: subversiune; subminare economică; manipulare și influențare psihologică a populației și a unor lideri. Acțiunile de spionaj ale Federației Ruse nu sunt îndreptate numai împotriva României ci și împotriva facilităților militare NATO găzduite de țara noastră. Federația Rusă acționează

permanent, proactiv și agresiv în direcția destabilizării statelor din flancul estic al NATO prin potențarea vulnerabilităților cu impact direct asupra securității naționale.

- *I.72. Tendințele negative persistente în plan demografic (scăderea ratei natalității și creșterea ratei mortalității)*

Scăderea demografică va continua, ca urmare a scăderii natalității și a deceselor provocate de COVID-19. De asemenea, criza economică care va urma pandemiei COVID-19 va descuraja familiile tinere în a face copii.

Tendința este din ce în ce mai evidentă, mai ales în ceea ce privește sporul natural. Reformele arbitrare și inconsecvența/incoerența statului în formularea unei politici publice în domeniu, au condus la permanentizarea stării de fapt.

Pe termen lung, descreșterea numerică a populației atrage dificultăți majore în a a sigura stabilitatea economică a țării cu implicații majore asupra capacității naționale de apărare și asigurare a securității naționale.

- *I.18. Fenomene grave, de natură geofizică, meteorologică ori asociate (inundații, cutremure, alunecări de teren etc.)*

Lipsa de analize sau analiza limitată a riscurilor climatice și a impactul devastator al producerii acestora cu influență directă asupra vieții umane.

Chiar dacă efectele acestor fenomene sunt reversibile, timpul de revenire la normalitate este dependent de vulnerabilități sau disfuncționalități de ordin intern (indecizia în realizarea de proiecte ample de contracarare a acestora: consolidări de clădiri, îndiguiri, oprirea tăierii pădurilor etc).

- *I.25. Degradarea mediului înconjurător, ca urmare a unor activități umane periculoase, dăunătoare sau iresponsabile (poluarea gravă, producerea unor pandemii etc.)*

Statisticile indică o criză climaterică accentuată la nivel global, datorită perpetuării unor metode învechite de uz industrial și managementului defectuos sau abuziv al resurselor. Creșterea gradului de aciditate a oceanelor reprezintă provocarea majoră care va genera o serie de efecte în lanț, parțial ireversibile: topirea calotei glaciare, destabilizarea

balanței ecosistemului global, inundarea zonelor de coastă și creșterea nivelului mărilor și oceanelor, strămutarea unor populații (se estimează o dinamică de relocare a peste 300 milioane de locuitori din zonele de coastă), extincția unor specii de viețuitoare, deșertificare, fenomene meteorologice extreme, crize alimentare, diminuarea resurselor de apă potabilă etc.

Lipsa unor politici publice care să prevină degradarea mediului ambiant va genera apariția unei noi tipologii de conflicte cu accent pe mutații demografice și acces la resurse de bază. Specialiștii atrag atenția asupra riscului reapariției de noi virusuri care au fost înghețate/conservate în calota glaciară în urmă cu milioane de ani. Odată cu topirea premafrostului este probabil ca umanitatea să se confrunte cu provocări pandemice necunoscute în istoria recentă. Distrugerea balanței ecosistemului global reprezintă o amenințare transnațională, iar România nu va fi exceptată de efectele sale.

Lipsa unor politici publice, determinate de potențarea și permanentizarea unor vulnerabilități-cheie determină accentuarea efectelor produse de degradarea mediului încurajator și care produc disfuncționalități economico-sociale grave pe termen lung, afectează direct viața, imposibil de remediat în caz de producere.

- 1.76. *Agresiuni informaționale din partea Federației Ruse (campanii mediatiche denigratoare, agresiuni informaționale din partea Federației Ruse (campanii mediatiche denigratoare, campanii de dezinformare etc.) la adresa unor lideri politici, membrii ai aparatului administrativ central sau local, lideri militari, responsabili pe linia apărării securității naționale, lidei de opinie etc.) din cauza amplasării unor elemente ale scutului antirachetă SUA în România*

Acțiuni specifice confruntărilor asimetrice generate de interesele divergente ale SUA și Federației Rusă cu privire la modul de poziționare geostrategică a României.

România, alături de Polonia, este principalul contestatar al agendei ruse în Europa de Est, fapt ce face din România țintă predilectă a agresiunilor informaționale ruse, fiind favorizate de

corupție, disponibilitatea unor actori sociali de a submina ordinea constituțională.

Agresiunile informaționale ale Rusiei sunt eficiente nu numai pe perioade de crize dar și în timpul campaniilor electorale.

- *I.28. Exercițarea iresponsabilă și ineficientă a puterii, de către actorii politici din România, în dezacord cu principiile democrației și cerințele respectării drepturilor omului*

Scăderea încrederii cetățenilor în ordinea constituțională, potențiala apariție a unor oameni politici/forțe politice cu o agendă anti-democratică și ineficiența politicilor publice.

Slăbirea coeziunii la nivelul UE și scăderea încrederii în capacitatea NATO de a-și exercita rolul de garant al securității europene a generat abordări ideologice disonante cu efecte asupra stării securității la nivel național.

Din cauza lipsei de profesionalism și de valori morale a clasei politice, vor continua acțiunile menite să afecteze principiile democratice și drepturile omului. Există premise pentru apariția unor actori politici populist, naționaliști sau chiar extremiști, care să exploateze starea de insatisfacție a populației, generată de insecuritatea socială la care este expusă.

- *I.30. Creșterea nivelului infracționalității la nivelul României*

Este direct proporțională cu nivelul scăzut de aplicare a legii. Structurile abilitate parcurg o perioadă grea, marcată de resursă umană calificată din ce în ce mai redusă numeric, de bugete inconsistente care să susțină operațiuni de anvergură. De aceea, nici resursele tehnologice necesare în acțiunile de contracarare a fenomenului nu sunt adaptate actualelor progrese tehnice.

Reducerea substanțială a veniturilor populației ca urmare a crizei economice generate de COVID-19 și disoluția autorității statului, coroborate cu întoarcerea în țară a unui număr mare de persoane predispuse la acte ilegale, vor genera creșterea infracționalității (jafuri, furturi etc).

Poate genera o cădere a ordinii publice, cu impact devastator, din punct de vedere economic, social și al funcționării instituțiilor statului român.

- *1.55. Agresiune militară convențională din partea Federației Ruse, îndreptată împotriva României, ca urmare a deciziei de amplasare a unor elemente ale scutului antirachetă SUA în România*

Plasarea României între interesele geopolitice divergente ale SUA și Federației Ruse la Marea Neagră este evidentă însă, probabilitatea de producere este redusă. O posibilă agresiune militară a Rusiei nu poate fi însă ignorată, mai ales că o reacție din partea NATO poate fi posibilă în minimum 24 de ore.

Din perspectiva documentelor programatice și ale declarațiilor oficiale din partea Federației Ruse, România poate a fi considerată o potențială țintă. Probabil că, Forțele Armate ale României nu pot să respingă (blocheze) o eventuală agresiune militară, declanșată de forțe de genul celor pe care le vedem în ultimul timp angajate în exercițiile militare ale Federației Ruse și nici nu pot să reziste până la o eventuală intervenție a aliaților (Art.5/Tratatul NATO).

- *1.82. Nivelul scăzut al rezilienței și spiritului civic al cetățenilor români (lipsa voluntariatului în gestionarea unor situații de criză în plan local – inundații, incendii etc.)*

Există foarte puține inițiative, care promovează educația și cultura de securitate la nivel național. Istoria recentă ne arată că trebuie să ne confruntăm cu o pandemie, pentru a conștientiza nevoia de implementare a unor mecanisme de răspuns la crize. Deficiențele privind avertizarea timpurie și comunicarea strategică în situații de criză, dar mai ales în pregătirea cetățenilor, indică existența unei disfuncții de comunicare între cei care conduc și cei conduși.

Se impune preluarea de bune practici de la partenerii externi, precum și atragerea de finanțări pentru implementarea unor proiecte de creștere a rezilienței și spiritului civic.

În condițiile unui mediu de securitate impredictibil, o condiție-cheie a supraviețuirii este construirea unei societăți reziliente – de la instiuții la indivizi, experiența societății

israeliene putând reprezenta un ghid de bune practici pentru a gestiona eficient „aterizările forțate”.

Nivelul scăzut al spiritului civic scade mult participarea populației la rezolvarea situațiilor de criză sau chiar s-o înrăutățească.

- *1.83. Migrația masivă a populației active, capabile de muncă și/sau înalt specializată (medici, asistente medicale, ingineri, profesori etc.)*

Pierderea populației active și înalt calificate reprezintă o problemă de interes național pentru România, țară de top în ce privește mărimea diasporei. Suprapunerea fenomenului migrației intelectuale peste sporul demografic negativ indică premisele unei crize de resursă umană la nivel național și, implicit, incapacitatea de a susține dezvoltarea unor sectoare-cheie. Pe de altă parte, procentul populației asistate social este mare, raportat la capacitatea economică a statului și la mărimea populației active. Acest fenomen va tinde astfel să genereze un decalaj de dezvoltare tot mai accentuat în raport cu alte state din UE.

Dezvoltarea economică în sectoare-cheie este afectată pe termen mediu și lung de fenomenul migrației masive a forței de muncă.

Pe fondul crizei economice generate de COVID-19 este de așteptat o migrare masivă a populației înalt specializate spre state din Europa de Vest și America de Nord. Acest trend va fi puternic influențat de modul în care statul gestionează efectele imediate și pe termen lung ale COVID-19.

- *1.90. Lipsa încrederii sau încrederea scăzută a cetățenilor români în instituțiile publice*

Lipsa de încredere în instituțiile statului este invers proporțională cu disponibilitatea cetățeanului de a contribui la asigurarea propriei sale securități.

Este rodul eșecului separației puterilor în stat, care transformă luarea oricărei decizii într-un act contestabil public, funcție de interesele unor grupuri de interese. Acest lucru conduce la lipsa coeziunii sociale. Fără cooperare interinstituțională reală, adaptarea la cerințele apărării colective și comune, nu poate fi realizată.

- *I.11. Impactul unor crize umanitare (criza refugiaților din Siria, din Fâșia Gaza etc.) asupra securității economice (cheltuieli generate de acceptul de a găzdui refugiați, conform convențiilor internaționale la care România este semnatară) sau securității societale (creșterea infracționalității din cauza prezenței unor infractori printre refugiați)*

Consecință a nesoluționării crizelor din astfel de regiuni (în Siria, durează deja de 9 ani) și a comportamentului cel puțin controversat al unor actori statali relevanți, fluxul migraționist generează insecuritate și instabilitate pe termen lung în Europa. În plus, facilitează discursul radical și apariția unor curente politice radicale.

- *I.24. Dependența accentuată de unele resurse care nu se regăsesc într-o proporție suficientă pe teritoriul României*

Limitarea/epuizarea resurselor reprezintă o realitate și în România. Lipsa investițiilor și a forței de muncă în anumite sectoare (în special cel agricol) determină dezechilibre în ceea ce privește consumul. Dacă adăugăm la acestea și risipa de resurse, potențialul de creștere economică are de suferit.

Nivelul insuficient al producției agricole în România cumulat cu o industrie alimentară subdimensionată (producem mai puțină hrană decât avem nevoie). Consum de petrol (produse derivate) mai mare decât rezervele pe care le deținem.

- *I.66. Campanii de dezinformare etc.) la adresa unor lideri politici, membrii ai aparatului administrativ central sau local, lideri militari, responsabili pe linia apărării securității naționale, lidei de opinie etc.) din cauza permiterii forțelor navale ale SUA să folosească facilitățile navale din portul Constanța sau facilitățile aeriene de la baza Mihail Kogălniceanu din județul Constanța*

Prezența SUA la Marea Neagră reprezintă un avantaj pentru România, iar adversarii SUA ar putea considera că această prezență poate fi anihilată prin dezinformare.

- *I.68. Acțiuni de propagandă și prozelitism, în scopul recrutării de membri și simpatizanți, derulate în România de către elemente radicale de extremă dreapta (anti-globaliști, anti-ACTA etc.)*

Apariția unor partide politice. care au adoptat ideologii neomarxiste și extremiste.

- *1.71. Traficul cu ființe umane, pe și/sau de pe teritoriul României, care să alimenteze rețelele de prostituție sau cerșetorie*

Este un factor de risc mai mult decât evident, pe fondul lipsei de educație a unor categorii sociale defavorizate și al ineficienței politicilor publice. Lipsa voinței politice în conturarea unei viziuni privind prevenirea și combaterea acestui fenomen denotă incapacitate instituțională.

Din nefericire, România este un contribuitor important la rețelele de prostituție și cerșetorie din Europa. Aceste activități afectează imaginea externă a României, dar și a diasporei.

- *1.84. Lipsa unor strategii eficiente de protejare a infrastructurilor critice (spitale, rețele de transport energie etc.)*

Lipsa unor strategii naționale de relansare a obiectivelor strategice. Pornind de la o nouă Strategie Națională de Securitate, trebuie dezvoltate strategii sectoriale, inclusiv de dezvoltare și protejare a infrastructurii critice, în concordanță cu principiile de la nivelul NATO și UE.

- *1.85. Lipsa unor reforme în învățământ care să permită racordarea educației la evoluțiile tehnologice și ale societății cunoașterii la nivel global*

Lipsa adaptării sistemului de învățământ la trendurile academice globale este generată atât de absența unei reforme coerente, cât și de subfinanțarea educației. Absența resurselor din educație reflectă în scorurile mici de cercetare-inovare, automatizare, inteligență artificială, digitalizare, competitivitate etc.

Analiza cost-beneficiu demonstrează că investiția în educație potențează direct dezvoltarea societății pe termen mediu și lung.

- *1.7. Implicarea în activități de crimă organizată (contrabandă, evaziune fiscală, spălare de bani etc.) a unor membri și simpatizanți ai insurgenței talibane din Afganistan sau Pakistan*

România nu este exceptată ca rută de tranzit, pentru contrabanda unor produse ilegale (în special stupefiante) provenite din Afganistan. Grupuri de crimă organizată autohtonă

și transnaționale au în vedere utilizarea rutelor de contrabandă, prin Marea Neagră spre vestul Europei.

- *1.58. Activitățile de spionaj ale serviciilor de informații din Ungaria, derulate pe teritoriul României*

Lecțiile învățate, în raport cu activitatea serviciilor de informații din Ungaria, după semnarea tratatului de la Trianon (4 iunie 1920), ne determină să avem în atenție direcțiile de acțiune ale spionajului maghiar pe teritoriul României.

- *1.75. Reapariția unor disensiuni între minoritățile etnice sau religioase din zona Balcanilor de vest și care pot genera în conflicte violente care să amenințe frontiera de sud-vest a României*

Apropierea Serbiei de Rusia și viceversa stârnește îngrijorări în spațiul euroatlantic. Orientările politice ale Serbiei se situează mai degrabă pe axa ortodoxă Moscova-Belgrad și pe culoarul eurasiatic. Tendințele sale, posibil revanșarde în plan regional, pot genera în viitorul apropiat conflicte de proximitate cu granița României, în Balcanii de Vest. Acest context nu poate fi tratat separat de agenda Rusiei în Marea Neagră, față de Ucraina, Moldova, Turcia și Bulgaria.

- *1.81. Gestiunea ineficientă a principiilor democrației, la nivelul separației puterilor în stat în România*

Măsurile populiste din România și tendințele de a politiza anumite instituții, cum ar fi Avocatul Poporului sau Curtea Constituțională au ridicat probleme cu privire la stabilitatea și predictibilitatea democratică a României în plan extern.

- *1.88. Lipsa unor reforme care să reglementeze piața muncii și asistența socială din România*

Fundamentată pe lipsa sau incoerența unei viziuni strategice, dublată de un nivel crescut de protecție socială, mai degrabă, încurajează nemunca.

- *1.91. Implicarea în activități de migrație ilegală (în scopul stabilirii în România sau tranzitării teritoriului național) de către membri și simpatizanți PKK (Partidul Muncitorilor din Kurdistan)*

Dar nu numai, pentru că sunt și state (Turcia, Libia) care încurajează migrația în UE, uneori foarte agresiv.

○ 1.98. *Activitățile de spionaj ale serviciilor de informații din Ucraina, derulate pe teritoriul României*

Serviciile de informații ruse și ucrainiene folosesc anumite structuri (ONG-uri, posturi TV și radio, edituri etc), ca și canale de influență, prin activități de promovare culturală sau științifică.

Analiza rezultatelor

Așa cum era de așteptat, la fel ca și în cazul respondenților din 2013, o analiză cantitativă a frecvențelor ne indică o prezență multiplă a unor indicatori în clasamente de mai sus, pe poziții și cu frecvențe diferite, motiv pentru care, a fost realizată și a doua etapă a prioritizării, prin ponderarea frecvenței indicatorilor stabilindu-se astfel frecvențele indicatorilor pe unul dintre cele zece locuri ale clasamentelor riscurilor și amenințărilor la adresa securității naționale.

Conform clasamentului frecvențelor ponderate⁵, primele zece locuri sunt ocupate de următoarele riscuri, amenințări și vulnerabilități la adresa securității naționale:

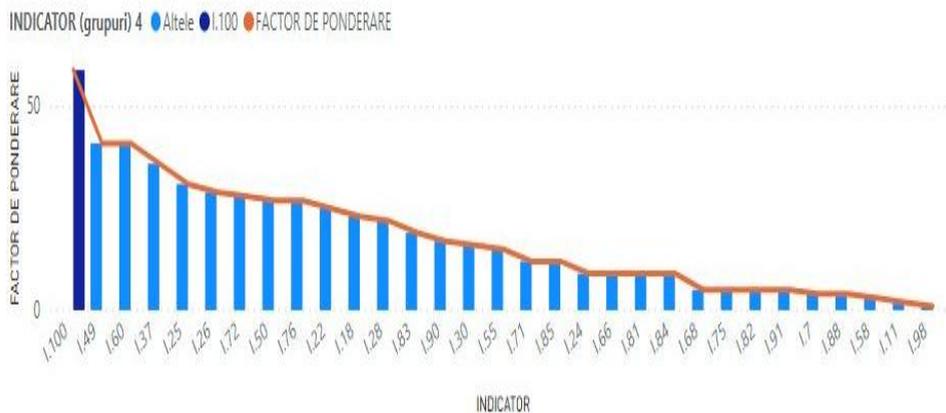


Figura 3: Distribuția indicatorilor în funcție de factorul de ponderare (Sursa: autorii)

⁵ Pentru locul 1 – valoare de ponderare 10, pentru locul 2 - valoare de ponderare 9, pentru locul 3 – valoare de ponderare 8 ... pentru locul 10 – valoare de ponderare 1. Factorul de ponderare a fost calculat prin însumarea valorilor obținute de fiecare indicator.

- I.100. Indicator nou, corelat cu manifestarea pandemiei COVID-19.
- I.49. Agresiuni informaționale (campanii mediatice denigratoare, campanii de dezinformare etc.) la adresa unor lideri politici, membrii ai administrației publice centrale sau locale, lideri militari etc., din partea unor actori interni (ONG-uri, partide politice, reprezentanți ai mass media etc.), din cauza aservirii acesora unor interese străine (ale Federației Ruse, Ungariei, Iranului, Ucrainei etc.).
- I.60. Activitățile de spionaj ale serviciilor de informații din Federația Rusă, derulate pe teritoriul României.
- I.37. Corupția în rândul funcționarilor din administrația publică centrală și locală din România.
- I.25. Degradarea mediului înconjurător, ca urmare a unor activități umane periculoase, dăunătoare sau iresponsabile (poluarea gravă, producerea unor pandemii etc.).
- I.26. Creșterea nivelului de insecuritate socială și persistența stării de sărăcie la nivelul claselor sociale din România.
- I.72. Tendințele negative persistente în plan demografic (scăderea ratei natalității și creșterea ratei mortalității).
- I.50. Agresiuni informatice din partea Federației Ruse asupra unor infrastructuri critice (rețele hidrografice, sectorul energetic, sectorul militar, administrativ etc.) ale României, din cauza permiterii forțelor navale ale SUA să folosească facilitățile navale din portul Constanța sau facilitățile aeriene de la baza Mihail Kogălniceanu din județul Constanța.
- I.76. Agresiuni informaționale din partea Federației Ruse (campanii mediatice denigratoare, agresiuni informaționale din partea Federației Ruse (campanii mediatice denigratoare, campanii de dezinformare etc.) la adresa unor lideri politici, membrii ai aparatului administrativ central sau local, lideri militari, responsabili pe linia apărării securității naționale, lidei de opinie etc.) din cauza amplasării unor elemente ale scutului antirachetă SUA în România.
- I.22. Lipsa de profesionalism a funcționarilor din administrația publică centrală și locală din România.

O analiză comparativă a clasamentelor respondenților pentru anul 2013, respectiv 2020 și a clasamentului experților ne indică

apariția constanță, ce-i drept pe poziții diferite, a unor riscuri, amenințări și vulnerabilități. De menționat că, în vreme ce riscul la adresa securității naționale generat de activitățile de spionaj ale serviciilor de informații din Federația Rusă derulate pe teritoriul României a „coborât”, în viziunea respondenților, de pe locul 6 (în clasamentul pentru anul 2013) pe locul 11 (în clasamentul pentru anul 2020), experții au poziționat acest indicator pe locul 3, în anul 2020.

Mai mult, se poate observa că această poziție de top cu privire la activitățile de spionaj ale serviciilor de informații din Federația Rusă, derulate pe teritoriul României corelează în clasamentul realizat de experți și cu alte amenințări din partea Federației Ruse precum agresiunile informaționale din partea Federației Ruse (poziția 2 și 9 din clasament) și agresiunile informatice (poziția 8 din clasament).

Analiza comparativă ne arată și evoluția ponderii intern/extern a riscurilor, amenințărilor și vulnerabilităților indicate de respondenți, respectiv de experți. Dacă doar două dintre primele zece poziții ale clasamentului pentru anul 2013 se refereau la riscuri generate de actori externi (Federația Rusă, respectiv elemente afiliate Al Qaeda), pentru anul 2020 doar vulnerabilitatea generată de dependența accentuată de unele resurse (gaz, energie etc.), care nu se regăsesc într-o proporție suficientă pe teritoriul României, era menționată de respondenți, experții plasează amenințările din partea Federației Ruse pe patru dintre cele 10 poziții ale clasamentului.

În opinia noastră, poziționarea Federației Ruse în clasament este de înțeles, date fiind acțiunile acestui stat, ulterior anului 2013, din estul Ucrainei și din Crimeea, poziția față de NATO, acțiunile hibride la adresa unor state, precum și evoluția arsenalului armatei ruse din acest interval de timp.

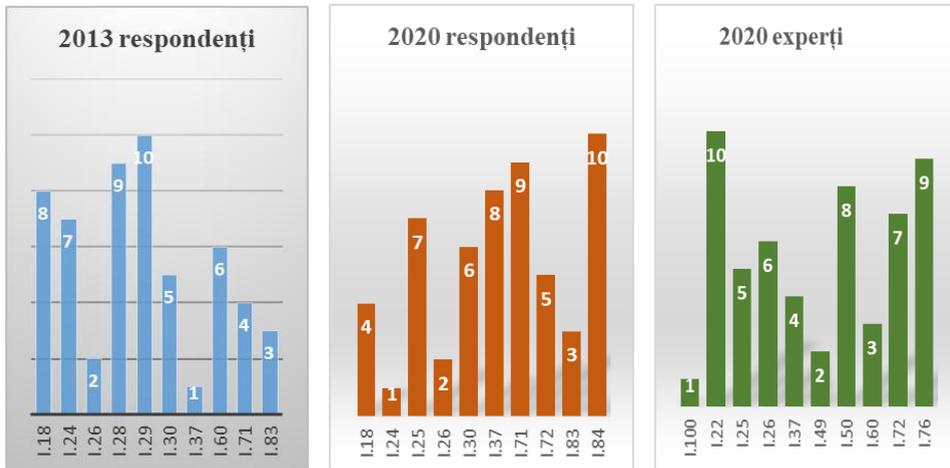


Figura 4: Clasamentul indicatorilor în funcție de respondenți și experți (Sursa: autorii)

În ceea ce privește restul pozițiilor din clasament, celelalte riscuri, amenințări, vulnerabilități sau disfuncționalități la adresa securității naționale a României sunt cele generate de acțiunile sau inacțiunile unor actori interni:

- corupția, exercitarea iresponsabilă și inefficientă a puterii, insecuritatea socială, sărăcia, migrația masivă a populației active, traficul cu ființe umane, infraționalitatea, fenomene grave de natură geofizică, meteoclimatică ori asociate (anul 2013);
- corupția, insecuritatea socială, sărăcia, migrația masivă a populației active, traficul cu ființe umane, infraționalitatea, fenomene grave, de natură geofizică, meteoclimatică ori asociate (perpetuându-se din anul 2013 până în anul 2020, în viziunea respondenților), tendințele negative persistente în plan demografic (scăderea ratei natalității și creșterea ratei mortalității), degradarea mediului înconjurător, ca urmare a unor activități umane periculoase, dăunătoare sau iresponsabile (poluarea gravă, producerea unor pandemii etc), precum și lipsa unor strategii eficiente de protejare a infrastructurilor critice (predicții ale respondenților pentru anul 2020);

- corupția, creșterea nivelului de insecuritate socială și persistența stării de sărăcie, degradarea mediului înconjurător, ca urmare a unor activități umane periculoase, dăunătoare sau iresponsabile (poluarea gravă, producerea unor pandemii etc), tendințele negative persistente în plan demografic (scăderea ratei natalității și creșterea ratei mortalității) și lipsa de profesionalism a funcționarilor din administrația publică centrală și locală.



Figura 5: Clasamentul final al indicatorilor în funcție de experți
(Sursa: autorii)

În cea de-a doua etapă de aplicare a metodei Delphi, experții au fost informați, că în urma prioritizării principalelor riscuri și amenințări la adresa securității naționale a României, doar 30 dintre cei 99 de indicatori se regăsesc, cu ponderi mai mari sau mai mici, în clasamentul întocmit, precum și faptul că, alți indicatori au fost formulați în prima etapă a prioritizării.

Ca atare, în scopul rafinării prioritizării, experții au fost rugați să ierarhizeze primii trei dintre cei 30 de indicatori rezultați, plus indicatorii de tip I.100 semnalati în prima etapă, în care pe locul 1 să poziționeze cel mai grav risc, amenințare sau vulnerabilitate.

În urma reprioritizării de către experți se poate observa că aceștia au decis să renunțe la a mai amplasa, în topul primelor trei cele mai grave riscuri, amenințări sau vulnerabilități, indicatori de tip I.100, analiza statistică indicând prezența în clasament a următoarelor riscuri, în urma ponderării⁶ amplasării indicatorilor pe una dintre cele trei poziții:

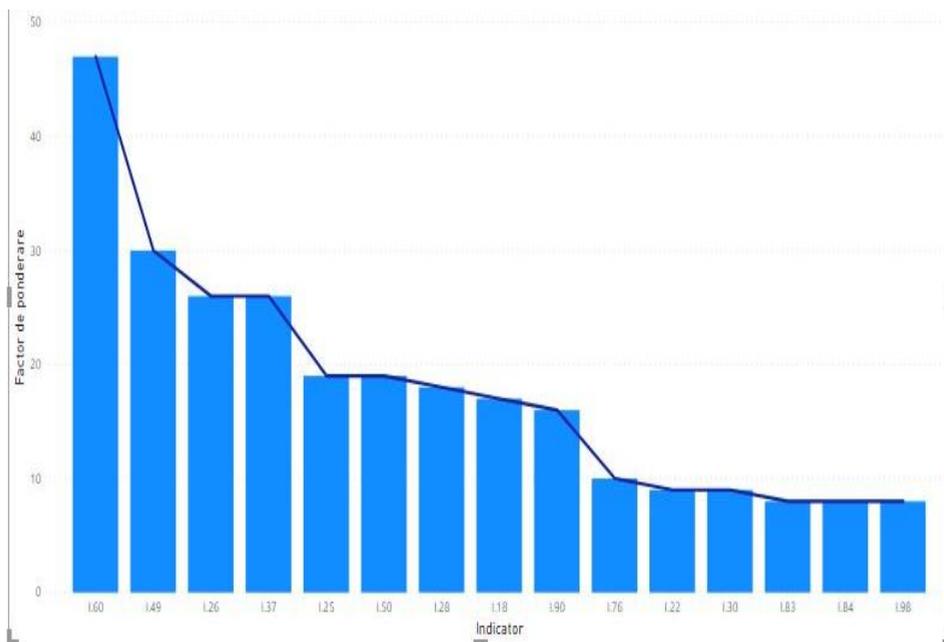


Figura 6: Graficul composit top 3 experți 2020
în funcție de frecvența indicatorilor și de factorii de pondere
(Sursa: autorii)

⁶ Pentru locul 1 – valoare de pondere 10, pentru locul 2 - valoare de pondere 9, pentru locul 3 – valoare de pondere 8. Factorul de pondere a fost calculat prin însumarea valorilor obținute de fiecare indicator.

- *I.60. Activitățile de spionaj ale serviciilor de informații din Federația Rusă, derulate pe teritoriul României.*
- *I.49. Agresiuni informaționale (campanii mediatice denigratoare, campanii de dezinformare etc.) la adresa unor lideri politici, membrii ai administrației publice centrale sau locale, lideri militari etc., din partea unor actori interni (ONG-uri, partide politice, reprezentanți ai mass media etc.), din cauza aservirii acesora unor interese străine (ale Federației Ruse, Ungariei, Iranului, Ucrainei etc.).*
- *I.26. Creșterea nivelului de insecuritate socială și persistența stării de sărăcie la nivelul claselor sociale din România.*
- *I.37. Corupția în rândul funcționarilor din administrația publică centrală și locală din România.*
- *I.25. Degradarea mediului înconjurător, ca urmare a unor activități umane periculoase, dăunătoare sau iresponsabile (poluarea gravă, producerea unor pandemii etc.).*
- *I.50. Agresiuni informatice din partea Federației Ruse asupra unor infrastructuri critice (rețele hidrografice, sectorul energetic, sectorul militar, administrativ etc.) ale României, din cauza permitterii forțelor navale ale SUA să folosească facilitățile navale din portul Constanța sau facilitățile aeriene de la baza Mihail Kogălniceanu din județul Constanța.*
- *I.76. Agresiuni informaționale din partea Federației Ruse (campanii mediatice denigratoare, agresiuni informaționale din partea Federației Ruse (campanii mediatice denigratoare, campanii de dezinformare etc.) la adresa unor lideri politici, membrii ai aparatului administrativ central sau local, lideri militari, responsabili pe linia apărării securității naționale, lidei de opinie etc.) din cauza amplasării unor elemente ale scutului antirachetă SUA în România.*
- *I.22. Lipsa de profesionalism a funcționarilor din administrația publică centrală și locală din România.*

Comparativ cu clasamentul frecvențelor ponderate, rezultat în urma prioritizării de către experți a celor 10 indicatori putem observa că aceștia și-au păstrat, în linii mari, opțiunile formulate, în elaborarea topului primelor trei cele mai grave riscuri și amenințări.

În plus, au fost semnalate ca fiind mult mai grave, comparativ cu prima prioritizare, următoarele riscuri, amenințări și vulnerabilități:

- 1.18. *Fenomene grave, de natură geofizică, meteoclimatică ori asociate (inundații, cutremure, alunecări de teren etc.), care se află pe locul 11, în urma primei prioritizări.*
- 1.28. *Exercitarea iresponsabilă și ineficientă a puterii, de către actorii politici din România, în dezacord cu principiile democrației și cerințele respectării drepturilor omului, care se află pe locul 12, în urma primei prioritizări.*
- 1.30. *Creșterea nivelului infraționalității la nivelul României, care se află pe locul 15, în urma primei prioritizări.*
- 1.90. *Lipsa încrederii sau încrederea scăzută a cetățenilor români în instituțiile publice, care se află pe locul 14, în urma primei prioritizări.*

În loc de concluzii

Securitatea și prosperitatea sunt termenii inseparabili ai aceleiași ecuații, ale cărei soluții sunt, printre altele, modernizarea radicală a sistemului de educație și valorificarea eficientă a potențialului uman, științific și tehnologic; creșterea bunăstării cetățenilor, a nivelului de trai și de sănătate a populației, precum și afirmarea și protejarea culturii, identității naționale și vieții spirituale.

Aceste obiective nu pot fi atinse decât prin operaționalizarea conceptului de „bună guvernare”, o condiție esențială a securității și prosperității, unitatea de măsură cumulativă prin care viața socială validează rezultatul alegerilor democratice, probează realismul programelor și capacitatea forțelor politice de a-și îndeplini promisiunile, cu stricta respectare a standardelor democratice, evaluând succesul măsurilor ce vizează combaterea insecurității, inechității și sărăciei și stabilește corecțiile necesare.

„Buna guvernare” nu poate fi realizată decât printr-o administrație publică eficientă, consolidarea independenței și eficienței justiției și creșterea încrederii populației în actul de justiție, precum și creșterea competitivității și a caracterului performant al activității economico-sociale prin asigurarea accesului tuturor cetățenilor la o educație de calitate, îmbunătățirea radicală a stării de sănătate a populației și realizarea unui nou echilibru social, printr-un sistem de

solidaritate capabil să garanteze securitatea economică, socială și de sănătate a tuturor participanților la proces.

În ceea ce ne privește, obiectivul cercetării noastre a fost de a oferi o priorizare a riscurilor, amenințărilor, vulnerabilităților și disfuncționalităților la adresa securității naționale a României, prin analizarea modului de raportare a unui eșantion de populație, nu reprezentativ pentru o cercetare sociologică cantitativă, dar semnificativ pentru una calitativă, la misiunile instituțiilor din sistemul de securitate națională, apărare și ordine publică din țara noastră, raportat la riscurile, amenințările, vulnerabilitățile și disfuncționalitățile la adresa securității naționale.

Această corelație între rezultatele celor două cercetări sociologice, derulate la o distanță de șapte ani una de cealaltă, ne îngăduie să afirmăm că investigații de acest gen se pot constitui într-un instrument de feed-back și predictibilitate sau analiză prospectivă pentru factorii de decizie.

Referințe

1. Barna, Cristian, Nicula, Valentin *Identifying risks and threats to Romania's national security. A sociological approach*, în *Proceedings of the XIXth international conference Intelligence in the Knowledge Society 2013*, pp. 271-290, ISSN 2392-7542, Editura Academiei Naționale de informații „Mihai Viteazul”, București, 2014.

2. *** Strategia de Securitate Națională a României. România Europeană, România Euro-Atlantică: pentru o viață mai bună într-o țară democratică, mai sigură și prosperă, 2007, www.presidency.ro

3. *** Strategia Națională de Apărare a României. Pentru o Românie care garantează securitatea și prosperitatea generațiilor viitoare, 2010, www.presidency.ro

4. *** Strategia Națională de Apărare a Țării pentru perioada 2015 – 2019. O Românie puternică în Europa și în lume, www.presidency.ro

TRANSLATING THE COPENHAGEN SCHOOL: A VIEW FROM ROMANIA

Valentin STOIAN*

Abstract

Transferring ideas, either from one country to another or between different professional environments, can lead, many times, to the erroneous reception of the theoretical and empirical implications of not only certain premises, but of entire schools of thought. Unfortunately, this is the case of the way the Copenhagen school was adapted and internalized in the Romanian military-academic environment.

The article aims to lay the groundwork for the rectification of errors generated by the way the Copenhagen school was adopted in Romania. It plans to overcome the simple idea that the Copenhagen school represented just an expansion of the concept of "security" and to unearth the ontological premises, the evolution of theoretical thought, as well as the implicit and explicit normative implications of the Copenhagen school. The article's main aim is to show that the initial theories of the founders of the Copenhagen school, as well as their further developments, are not adequate to being used in a military-academic environment and that the attempts to use them rely on a fragmentary and disparate adoption of some ideas. The central ideas of this school are more relevant for the civilian academic environment, especially political science, which treats the idea of "democracy" as a fundamental concept and explores the way to reach the desirable political regime.

Keywords: *Copenhagen school, Romanian military-academic environment, theoretical thought.*

Introduction

Transferring ideas, either from one country to another or between different professional environments, can lead, many times, to the erroneous reception of the theoretical and empirical implications of

* Researcher PhD, within "Mihai Viteazul" National Intelligence Academy, stoian.valentin@animv.eu

not only certain premises, but of entire schools of thought. Unfortunately, this is the case of the way the Copenhagen school was adapted and internalized in the Romanian military-academic environment.

In both military-academic milieus and in the public space, the term “Copenhagen School” has been employed. However, on these occasions, a number of mistaken uses of the fundamental principles as well as of the empirical results generated by the research associated with this program could be observed. The way this school of thought has been understood in the Romanian military-academic environment should be open to rectification.

The article aims to lay the groundwork for the rectification of errors generated by the way the Copenhagen school was adopted in Romania. It plans to overcome the simple idea that the Copenhagen school represented just an expansion of the concept of “security” and to unearth the ontological premises, the evolution of theoretical thought, as well as the implicit and explicit normative implications of the Copenhagen school. The article’s main aim is to show that the initial theories of the founders of the Copenhagen school, as well as their further developments, are not adequate to being used in a military-academic environment and that the attempts to use them rely on a fragmentary and disparate adoption of some ideas. The central ideas of this school are more relevant for the civilian academic environment, especially political science, which treats the idea of “democracy” as a fundamental concept and explores the way to reach the desirable political regime.

From a conceptual point of view, the development of constructivist and critical-constructivist security studies generated a vast enough material to make a single, even synthesis article, impossible. This is the reason for which the article will distinguish between the conceptual elements of the Copenhagen School, which it will rely on. According to Ole Waever (2003), the theoretical elements that define one’s belonging to this school are “1. the theory of securitization 2. the idea of security sectors 3. the concept of a regional security complex”. The article’s main focus is the theory of securitization and the way it has evolved in the literature. Therefore,

the selection will be done on the basis of the topic approached and less on the work of a certain specific author. The article will canvass a wide number of authors and will describe the development of the theory of securitization, which represents the main axis of the thought of the Copenhagen school. The development of this theory will be traced and two "generations" of theoreticians will be identified.

The first part of the article will discuss the ontological aspects of the Copenhagen school. The main claim of this section will be that the theoretical innovation of the Copenhagen school is the switch from a positivist ontology to a critical-constructivist one, which is implicitly presented in the early works of the Copenhagen school and explicitly elaborated in their further work.

The second section of the article will discuss the conceptual differences between the different generations of the Copenhagen School. The first generation was criticized because it only focused on speech acts and did not include aspects such as public policies, images or popular movies as tools of securitization. Moreover, another relevant criticism addressed to the first generation of securitization researchers was that they did not consider the role of the audience and the reasons for which an attempted securitization succeeds or fails. This argument shifts the focus from the securitizing agent to the audience which accepts or rejects a securitization move.

The last section will focus on the normative implications of securitization theory. These are explicitly accepted by the initial developers of the theory in their late work. By this point of the development of the literature, a general consensus was reached that the main aim of constructivist analysis is the de-securitization of certain issues. Thus, as Waever (2011) mentions, the Copenhagen school's main aim is to "exit security" and to solve political problems through deliberative means, integrating a wide deliberation of citizens. This section will critically discuss a contemporary attempt to employ critical constructivism and to integrate it into intelligence analysis. The main argument of this analysis is that this attempt relies on the taking out of context of the ontological premises of the Copenhagen School and on the selective use of its theoretical premises.

The ontological premises of the Copenhagen School

The following section will describe the two relevant directions of the Copenhagen School: the theory of securitization and the theory of the sectors of security. As this section will show, although in the initial works, such as *Peoples, states and fear* (Buzan, 1991[1983]), the theorists of the Copenhagen school suggested a simple extension of the idea of security (thus arguing that the problems of the individual are "security problems") and operated with a relatively classical idea of security, this conception was consistently modified as the theoretical thought of the authors of the Copenhagen school evolved. Thus, already at the end of the previous century, Ole Waever and Barry Buzan stopped using the framework of "security in different sectors" and employed the concept of "securitizing sectors" (Waever, 1999).

People, States and Fear is a work written during the Cold War and revised after the end of this conflict. Although it is generally, though incorrectly, considered the fundamental work of the Copenhagen School, in itself it represents a major contribution to the field of security studies. However, across this work, "security" remains something objective, either a state of fact or an opinion of the individual about that state of fact. On the other hand, in this work, Barry Buzan asks the question "The security of whom?", and replies that the security of the individual is at least as important as the security of the state. Furthermore, the idea that the nature of the threat can be different according to the sector from which it arises is also formulated in *People, States and Fear*. Thus, the theoretical groundwork which will later define the reception of the Copenhagen School was laid in 1983, leading many authors to "forget" about the parallel evolution of the theory of securitization.

Regarding individual security, Barry Buzan argues that: "*Security for individuals, however, cannot be defined so easily. The factors involved – life, health, status, wealth, freedom – are far more complicated, not infrequently contradictory, and plagued by the distinction between objective and subjective evaluation. Many of them cannot be replaced if lost (life, limbs, silitus), and cause-effect relationships with regard to threats are often obscure.*" (Buzan 1991[1983], p. 18)

Moreover, in his 1983 work, Buzan accepts the idea that individual security can be threatened, among others, by its own state: *"The individual citizen faces many threats which emanate either directly or indirectly from the state and which not uncommonly may occupy an important place in the person's life. Such threats can be grouped into four four general categories: those arising from domestic law-making and enforcement; those arising from direct political action by the state against individuals or groups; those arising from struggles over control of the state machinery; and those arising from the state's external security policies."* (Buzan 1991[1983], p. 20-25)

Concerning the nature of the threat, Buzan argued that there can be multiple threats, both to the individual and to the state and that these can come from different sectors of life. Thus, in the military sector, the main threat is the possibility of an invasion but also the negative consequences this might have on the citizens. In the political sector, the threats to a state are political ideas fundamentally opposite to its principle of organization but also political terrorism that affects the individual. With regard to economic security, the main threats are the economic weakening of the state, the threat of economic sanctions from another state as well as the threat of restricting vital resources. On the other hand, these can affect the individual, who can lose his standard of living, can suffer different forms of deprivation and can be forced to undertake humiliating activities for it. The environment represents, according to Buzan's 1983 view, another relevant sector of security, given that it generates threats to the individual (through environmental pollution) but also to the state (which needs to cover the consequences of this pollution. (Buzan 1991[1983], p. 73-80)

The third "referent object" of security emerges in a later work of the theoreticians of the Copenhagen School, entitled *Identity, Migration and the New Security Agenda in Europe*, published by Barry Buzan and Pierre Lemaitre in 1993. Thus, if in Buzan's original work societal security was only a part of state security, in 1993, society became itself a referent object of security. Society is transformed into a referent object of security by taking into consideration the possibility that identity, seen as the social "glue" binding a community together, is threatened by another religious, ethnic or supra-national identity

(McSweeney 1996). Thus, in the first years after the publication of the works of the theorists of the Copenhagen school, both its representatives and its commentators argued that its main contribution to the debate on security studies is that it asked the question "security for who?" (Baldwin 1997).

Buzan's and Waever's decision to approach society as a "referent object of security" led to a heated exchange between Bill McSweeney, on the one hand, and Ole Waever and Barry Buzan, on the other (McSweeney, 1996; 1998, Buzan and Waever, 1997). The first (the one who invented the concept of the "Copenhagen School"), accused the latter two of employing a far too "objectivist" approach to identity and argued that it had to be treated as a social construct, as the literature did. On the other hand, Buzan and Waever, denied the accusations and stated that they treated identity as socially constructed but that security phenomena emerged when different attempts to construct security clashed. Further, McSweeney's answer was that these forms of theorizing (where identity is treated as a "referent object" similarly to the state), exposed the authors of the Copenhagen School to the accusation of "methodological holism", which, if they accepted, they had to justify the supra-individual entities they considered relevant (McSweeney, 1998, p. 139).

The importance of these debates during the first generation of the Copenhagen school, as well as the parallel development of securitization theory, determined David Baldwin to state, in 1997, that: *"In sum, to the extent that the new thinking about security focuses on conceptual issues rather than empirical or normative issues, not much is new. Most of the 'new ideas' about security can be accommodated by the conceptual framework elucidated by Wolfers in 1952. The United Nations Secretary-General recently called for a 'conceptual breakthrough' which goes 'beyond armed territorial security' to include 'the security of people in their homes, jobs and communities."* (Baldwin, 1997, p. 23)

The main argument of this article is that the central innovation of the Copenhagen School, which was later taken over by other constructivist or critical schools of thought is the *intersubjective nature of security* (Waever, 2003). Both Waever (1995, 2003, 2011), Waever, Buzan and de Wilde (1998), as well as other authors such as Stritzel

(2007), McDonald (2008), or Meszaros (2017) argue that security represents an inter-subjective construction between the securitizing actor and the audience which receives the securitizing message. Thus, in contrast to the classical constructivist (Katzenstein, 1996; Wendt, 1999) or neo-realist (Diesen, 2015) conception, in the view of the Copenhagen School, identity is not only a factor that explains security phenomena, but also the content of threats is a process subjected to social construction through a dialectical relation between a securitizing actor and an accepting audience.

Throughout his work, Waever's central argument is that, if under different theories, the content of "security" does not vary, but the factors that explain security phenomena do (constructivists offer a privileged status to identity while realists to determinants of power), in his theory, the very content of "security" is variable. Waever claims that he is the first author who fully rejects Arnold Wolfer's (1952) vision that security amounts to lack of threats and a subjective opinion that these are absent (Wolfer, 1952 apud Waever, 2003). Moreover, Waever argues that previous debates on security have begun from an erroneous premise: that the relevant debate concerns the existence and causality of threat, the correct or erroneous perception of it and, at most, the relevant referent object of security (either the state or the individual). Waever (2003, p. 32) looks to distinguish his own theory from the previous ones and to reject the idea that his view only focuses on the "subjective side of security". In Waever's view, there is no such thing as an "objective side" or a "subjective side" of security – there is no such thing as a "real" threat unless it has been "spoken" by a relevant actor and "accepted" by the relevant audience. That is why, in Waever's view, this threat is not "real" except for the two relevant groups.

A central element of securitization theory (at least in its initial version) is the claim that language plays a performative role (Waever, 2003; Stritzel, 2007; McDonald, 2008a). This idea, taken up from the British philosopher J. Austin argues that some statements, when spoken by certain actors (speech acts), under relevant conditions, have the effect of creating a certain reality rather than describing a reality outside the speech act. The examples in the literature are those of

pronouncing marriage or apologizing, which produce effects only through the utterance of the speech by a relevant authority.

The following section will exemplify definitions of security by the theorists of the Copenhagen School, as well as some relevant criticisms, which all show that these conceive threats in an inter-subjective fashion. Both in 1989 (Waever, 1989) when Waever, for the first time, defended the idea of securitization, and in 1995 when Waever defined security as a speech act through which a certain actor lifts a problem from the sphere of "normal politics" and takes it to the sphere of "extraordinary politics", security is defined as "inter-subjective": *"What is then security? One can view 'security' as that which, is in language theory called a speech act: it is not mainly interesting as a sign referring to something more real – it is the utterance in itself that is the act: by saying it, something is done (like betting, giving a promise, naming a ship). By saying 'security' a state-representative moves the particular case into a specific area; claiming a special right to use the means necessary to block this development, but paying the price of some loss of prestige by needing to use this special resort."* (Waever, 1989, p. 4; 1995, p. 7)

Furthermore, Buzan, Waever and de Wilde argue that: *"It is when an issue is presented as posing an existential threat to a designated referent object (traditionally, but not necessarily, the state, incorporating government, territory, and society). The special nature of security threats justifies the use of extraordinary measures to handle them. The invocation of security has been the key to legitimizing the use of force, but more generally it has opened the way for the state to mobilize, or to take special powers, to handle/existential threats. Traditionally, by saying "security," a state representative declares an emergency condition, thus claiming a right to use whatever means are necessary to block a threatening development."* (Buzan, Waever and de Wilde, 1998, p. 21)

and that: *"Security" is the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics"* (Buzan, Waever and de Wilde 1998, p. 21)

Furthermore, in 2003, Waever claims that: *"The designation of the threat as existential justifies the use of extraordinary measures to handle it. The invocation of security has been the key to legitimising the*

use of force, and more generally opening the way for the state to mobilise or to take special power – e.g. using conscription, secrecy, and other means only legitimate when dealing with ‘security matters’. (Waever, 2003, p. 9)

In a later article, Waever (2011, p. 470) distinguishes his own theory from previous ones. Firstly, he claims that previous theories have attempted to "widen" the concept of security, either through the expansion of the reference object or through the introduction of new "sectors", where phenomena were described as "security phenomena". However, *“it was how securitization theory ‘solved’ the widening impasse. Until the invention of the concept of securitization, ‘widening security’ had to specify either the actor (the state) or the sector (military), or else risk the ‘everything becomes security’ trap. Securitization theory handled this problem by fixing form: whenever something took the form of the particular speech act of securitization, with a securitizing actor claiming an existential threat to a valued referent object in order to make the audience tolerate extraordinary measures that otherwise would not have been acceptable, this was a case of securitization; in this way, one could ‘throw the net’ across all sectors and all actors and still not drag in everything with the catch, only the security part.”* (Waever, 2011, p. 469)

The intersection between securitization theory and sectorial security is already visible in 1998. If *People, States and Fear* employs the idea of sectors of security and does not use securitization theory, already in *Security: a New Framework for Analysis*, the way security sectors are conceived is radically different. Thus, when presenting the theoretical framework of inter-subjective security, certain authors claim that there is relevant difference between the military sectors, where "securitization is institutionalized" through the existence of a military and intelligence bureaucracy, which is, many times, "separated from normal politics" (Buzan, Waever and de Wilde 1998, 28) and the environment sector, which calls for securitization. The differences between the two are significant, considering that the idea that these are "security issues" emerged far later. Thus, the authors of *Security: a New Framework for Analysis* conceive sectorial security very differently in 1998 as opposed to 1983, by introducing the idea of inter-subjective security within these sectors.

In 1999, Waever replied to the critique of Johann Eriksson (1999), who argued that, through the simple fact that it addresses sectorial security; the Copenhagen school is an integral part of the securitization processes. In his reply, Waever argued that the central claim of the Copenhagen School theory was that it represented the combination between securitization theory (which allowed for ascertaining whether security phenomena existed or not) and the conception of sectorial security. According to Waever, "the presentation of a sector does not mean that economic security exists, or that it is widespread and legitimate. The set-up with five sectors is an analytical net to trawl through existing security discourses to register what is going on. Whether we find that there is a lot of securitization in the environmental sector, is not a product of the sectorial approach, but of the actors' practices" (Waever, 1999, p. 335).

The second generation of securitization theorists

If the first generation of securitization theorists aimed to define the central direction of the process, the authors of the second generation offered several criticisms to the thinking of the previous one. The first set of criticism was that the authors of the first generation emphasized the receiving audience too little and did not focus enough on the enabling conditions of securitization. Further, the second generation authors stated that it was not necessary for securitization to occur through speech acts, but could take place through different forms of representation.

The first and most important criticism addressed to the first generation securitization theorists was that they did not take into consideration the audience when discussing securitization. Thus, it was claimed that a successful speech act was not only the act which designated a certain situation as being exceptional, but it was necessary for this statement to be accepted by a relevant audience. This audience legitimized the political actor when "exiting" "normal politics". The success of this statement depends on whether the securitizing actor fulfills several enabling conditions. According to Balzacq (2011, p. 1), the view according to which securitization is a process of accepting a certain speech act is called the "sociological view of security", while

those that subscribe to the idea that only the speech act is relevant are called the supporters of the "philosophical conception of security".

Generally, the supporters of the sociological view of security look at both the speech act and the accepting audience (McDonald 2008). The conditions under which a securitization act is successful are examined. These conditions pertain to both the author of the securitizing act as well as to the accepting audience. The relevant condition is that the securitizing speech act accesses already existent representations of the threat and only slightly modifies realities that are already "known" by the audience to whom the securitizing act is addressed.

A relatively simple form of the concept of facilitating conditions can be found in *Security: a new framework for analysis*

1) *the demand internal to the speech act of following the grammar of security,*

2) *the social conditions regarding the position of authority for the securitizing actor – that is, the relationship between speaker and audience and thereby the likelihood of the audience accepting the claims made in a securitizing attempt, and*

3) *features of the alleged threats that either facilitate or impede securitization* (Buzan, Waever and de Wilde 1998, 33).

Thierry Balzacq, one of the main theorists of the second wave of securitization, argues that it is not enough for the speech act to be considered by itself, but that an analysis of the context is required to understand if a certain speech act was successful or not. According to Balzacq (2005), a securitizing act can be analyzed according to a framework composed of five variables, two of them pertaining to the actor analyzed and three pertaining to the securitizing act and how it is deployed. According to Balzacq, the relevant aspects regarding the agent are: the power position and his personal identity, the social identity of the actor and the nature of the target audience, especially if opposing or contesting discourses exist. Regarding the securitization act itself, Balzacq identifies two relevant variables which can lead to the success of securitization – if the speech act is done according to the correct grammatical rules and if it employs relevant "heuristic artifacts"

such as metaphors, stereotypes and relevant analogies (Balzacq, 2005, p. 179-180).

Thus, according to Balzacq *“This means that the success of securitization is contingent upon a perceptive environment. Therefore, the positive outcome of securitization, whether it be strong or weak, lies with the securitizing actor’s choice of determining the appropriate times within which the recognition, including the integration of the ‘imprinting’ object – a threat – by the masses is facilitated.”* (Balzacq, 2005, p. 182)

A more extended and more relativistic version of securitization theory is defended by Holger Stritzel. He criticizes Buzan, Waever and de Wilde, and argues that, although they take a step ahead by accepting the idea that context is relevant for securitization, they do not analyze context by taking into consideration discourses present in society and the interaction between each securitizing act and already existent power relations. According to Stritzel, the relevant conditions for the analysis of securitization are:

These dimensions correspond with a structurationist understanding of power as the relatedness of

(1) the existing discourse, constituting the performative power and the meanings of security articulations, and

(2) the positional power of actors, influencing the process of defining meaning by enacting particular threat texts and/or shaping the existing discursive context. Conversely, the performative force of a threat text can help constitute or change existing discourse coalitions and/or change an existing discourse, thereby reconfiguring existing relations of power. Influencing the process of defining meaning is always marked by acts of translation of a certain threat text into an existing discourse. The better the compatibility of the articulated text/textual structure and the existing discourse (i.e. its ‘resonance’) and the better the positional power of securitizing actors, the easier it is for them to establish their preferred individual text as a dominant narrative for a larger collective (Stritzel, 2007, p. 370).

Balzacq (2011, p. 2) employs concepts inspired by the work of Pierre Bourdieu and Michel Foucault to describe the role of context in the process of securitization. According to him, the same act of

securitization differently influences audiences with different *habitudes*. The concept of *habitus* is derived from the theorizing of French sociologist Pierre Bourdieu, who defines it as a set of practices and attitudes specific to a professional group, which are practiced consciously or unconsciously. Furthermore, in Balzacq's view, securitization is the work of the "dispositif", a Foucauldian concept which designates power practices and mechanisms, as well as actors and practices that support them. According to Balzacq "*securitization amounts to practices that instantiate inter-subjective understanding through the habitus inherited from different social groups. The dispositive joins these practices together*". (Balzacq, 2010; 2011, p. 2)

Paul Roe (2008) analyses the role of audience in the acceptance of a securitization act. He shows that the former British Prime minister, Tony Blair identified Saddam Hussein's Iraq as a threat before two audiences: the British Parliament and the British Public. Although both audiences accepted the identification, Blair was only able to obtain the agreement of Parliament in order to intervene in Iraq. This securitization was only "half successful" because Blair achieved the mobilization of Parliament through the invocation of threatening images, but did not do the same for the general public, who had a negative opinion on American military intervention (Roe 2008).

Adam Cote's (2016) synthesis article analyses 32 other articles on securitization practices. Cote argues that, although the classical formulation of securitization theory only focuses on the securitizing agent and treats the audience as passive, empirical studies offer a different view. According to Cote, the audience of the securitizing speech act has been treated, in empirical studies, as an active actor, being the "person/persons or group(s) that can authorize the securitizing actor's view and to legitimate the treatment of a particular problem as a security practice (Cote 2016, 8). According to Cote, empirical studies present: *For example, the empirical literature contains instances in which audiences actively challenged, questioned, and/or supported claims made by the securitizing actor (Bright, 2012; Lupovici, 2014b; Salter, 2008; McInnes and Rushton, 2013), or undertook independent actions to modify, bolster, or destabilize security meanings, prompting engagement by securitizing actors (Bright, 2012; Wishnick,*

2010; Salter, 2008) and creating important effects on securitization outcomes and legitimized security policies. (Cote, 2016, p. 10)

Cote's conclusion, based on analysing 32 articles, is that although theoretical works treat practitioners as a passive actor, which does not influence the securitizing process, empirical works have a very different approach, showing that the audience can accept or reject a securitizing speech act.

Another criticism addressed to the first generation of Copenhagen School theorists concerns how securitization takes place. If, traditionally, the argument was that securitization takes place through a speech act, which could be accepted by the relevant audience, this was contested and an argument was put forward that images or public policies, that treat some issues as "security issues", also represent "tools of securitization".

For example, Michael Williams (2003) argued that the communication space radically changed, especially after the 9/11 attacks. He claims that images of terrorism (the repeated presentation of the 9/11 attacks) and migration (the representation of migrants as people who want to illegally enter the London-Paris Eurostar trains) generated a context in which securitizing speech acts were more easily accepted by the audience. Unlike Lene Hansen (2006), Williams remains faithful to the ideas of the first generation of the Copenhagen School, according to which securitization happens through a speech act, but adds that its effect is influenced by the context created by certain images.

Lene Hansen (2006) understands securitization through images far more strongly. According to her, images do not have the simple role to create the context in which securitization happens, but are, themselves, an act of securitization. Hansen is inspired by the post-structuralist idea according to which discursive speech acts articulate the Self through the definition of the Other, and thus amount to a form of othering. Given that positive connotations are attached to some referent objects and negative associations are given to others, the latter are denied legitimacy and are considered "security issues". Hansen analyses the Danish cartoon crisis of 2006 (when a wide circulation newspaper published cartoons showing Mohammed as a terrorist), and shows how these cartoons, as well as the comments that followed,

amounted to an act of "othering" of Muslims, through the association of Islamic culture with authoritarianism, patriarchy and medieval forms of behaviour while associating Danish values to democracy, gender equality and freedom of expression (Hansen, 2006, p. 10). In Hansen's view, this contributed to the extent of the cultural conflict that followed the Danish cartoon crisis through limiting the potential replies to the Muslim criticism against the cartoons.

Thierry Balzacq (2007) argues that the European Union's internal security policies, especially the creation of the three databases: SIS, VIS and Eurodac represent a form of securitization through public policies. According to it, some contexts do not require a speech act from a securitizing actor or the acceptance by the audience. In some cases, the securitizing actor does not need to perform a speech act due to having legislative power which allows him to adopt policies through which certain issues are taken outside "normal" politics and are "assigned" to security practitioners. Balzacq discusses the case of securitization of migration from outside the European Union, showing how the three databases allow an extended surveillance of this phenomenon and how European elites adopted this policy without consulting or receiving the agreement of the European public.

The normative implications of the Copenhagen school

Although the theory of securitization is seen as an explicative theory (describing how certain social phenomena take place), a set of authors argued that it amounts to a normative theory (includes value judgments on what is morally right and politically desirable). The literature argues that a correct understanding of securitization theory is that it implies the desirability of de-securitization, that is the removal of as many aspects from the sphere of the "exceptional" and bringing them back to "the political", which is defined as a part of social life governed by slow procedures and extended debates. This trail of thought can be found in a series of works by Ole Waever, but also of other interpreters of securitization theory.

The first mention of the idea that de-securitization is preferable to securitization can be observed in *Security: a New Framework of Analysis*. According to the book's three authors, a securitized situation is

seen as undesirable, unlike normal politics, which relies on rules and procedures and does not treat some aspects as exceptional. Thus, “de-securitization is the optimal long-range option, since it means not to have issues phrased as threats against which we have countermeasures but to move them out of this threat-defence sequence and into the ordinary public sphere” (Buzan, Waever, de Wilde 1998, p. 29).

Waever expands this argument in a 2011 article and claims that securitization theory can reject both meta-theoretical criticisms and explain its own normative commitment. From a meta-theoretical point of view, securitization theory was criticized by those that argue that the focus on the speech act tends to ignore other ways of “instantiating security”. Waever (2011, p. 469) argues that securitization theory has the necessary resources to integrate other forms of securitization than that done through speech acts. Furthermore, from the point of view of the normative implications of the theory, Waever claims that the theory “prefers” de-securitization, but that some concrete situations can “demand securitization”. Furthermore, Waever shows that, from the way the theory is built, the negative effects of securitization are highlighted such as the “logic of necessity, the restriction of choice, the transfer of power to a restricted elite”, but also the fact that the act of securitization can “help society solve important problems through the mobilization of attention and resources” (Waever, 2011, p. 469).

Within the same article, Waever comments on the main premises of securitization theory and argues that it has a “Schmittian concept of security and an Arendtian concept of politics” (Waever 2011, p. 470). This explains in a simple, but concise fashion, the fact that securitization theory contrasts an exceptional situation, associated with the views of Carl Schmitt, who believed that politics is a permanent conflict between friends and enemies, that universal laws cannot be applied and that the only real political act is the suspension of universal laws by the sovereign and the “exit” from the realm of law into the realm of pure will, with the normal situation where politics is undertaken according to traditional procedures. According to Arendt, who supports a classical liberal view, “politics” can only take place between equal individuals who deliberate in the public space, by using reason and attempting to persuade other through arguments.

Paul Roe (2012) synthesizes the available literature and shows the main arguments in favour of de-securitization. Roe argues that the literature can be divided in two: authors who support the claim that de-securitization is good by itself, as it removes aspects from the "empire of the exceptional" rely on the premise that deliberation is intrinsically superior to "decisionism". On the other hand, there are a series of supporters of the claim that the morality of de-securitization has to be evaluated according to its result (authors that have a utilitarian view on securitization): if, for example, a problem is extremely urgent and approaching it as exceptional can lead to finding a solution and this involves only minor individual rights violations, then securitization is morally desirable. On the other hand, as Roe shows, a series of authors such as Claudia Aradau and Columba Peoples argued that any securitization of a problem can lead to insecurity for other groups. According to those who share this view, only the radical "politicization" of problems is acceptable. (Roe, 2011, p. 261)

The greatest supporter of the utilitarian approach to de-securitization is Rita Floyd. Across several works (2007, 2008, 2011, 2015) she argues that the theories of the Copenhagen school are clearly normative but that the morality of a securitization depends on its degree of usefulness and on the intensity of a "real" threat which a speech act securitizes. Furthermore, Floyd argued that the securitizing speech act has to be judged by itself and rejects the claim according to which its acceptance by an audience is necessary in order to have a successful securitization. Floyd outlines a theory of "just" securitization and suggests a set of criteria according to which the justice of a securitization act can be appraised.

Floyd proposes the first version of the principles of just securitization in 2011 and expands and clarifies them in 2015. Thus, according to her, in order for securitization to be just:

1. *There must be an objective existential threat to a referent object, which is to say a danger that threatens the survival of either a political or social order, an ecosystem, a non-human species or a group of human beings.*

2. *Referent objects are entitled to defend themselves or are eligible for defensive assistance if they are morally justifiable [...] Political and*

social orders need to meet a minimum level of basic human needs satisfaction. Ecosystems and non-human species, in turn, need to make a contribution to the human needs of a large group of people.

3. The right intention for securitization is the just cause. The securitizing actor must be sincere in his or her intentions to protect the referent object they themselves identified and declared

4. The good gained from securitization must be judged greater than the harm securitization is expected to entail and the only relevant good for proportionality is the good contained in the just cause.

5. Securitization should not lead to more insecurity than it aims to solve, and of the options available the one that causes, or is expected to cause, the least insecurity should be chosen (Floyd 2015, 3)

Thus, it can be easily argued that the central idea of the Copenhagen school is that democratization is better than securitization, that widening the debate is more relevant than its quick resolution and that the involvement of a large number of actors is desirable, as opposed to the limiting of those who have access to a decision.

Claudia Aradau (2004, 2008, 2010, and 2015) argues in favour of a stronger concept of securitization. She claims that securitization theory is a truly normative one, in the sense that the use of the term "securitization", even with the aim of de-securitization, leads to the securitization of something. According to Aradau, the correct way of thinking about de-securitization is the "politicization" of decision spaces that have been "bureaucratized" or "securitized" until now, as well as the expansion of Universalist politics to include all people in a single political community. Aradau analyzes three cases which achieved this desideratum: the protests against the Iraq war, undertaken under the slogan of "not in my name" (Aradau, 2004), the statements by Brussels sex workers who claimed that European leaders do not speak in their name and that they do not need to be "protected" (Aradau, 2008) and the actions of a nomadic Roma group in France, who cleaned their own camp and, thus, defied the discourse on the "dirtiness" of this ethnic group. Aradau's main argument is that de-securitization does not necessarily take a discursive form, but that some actions, usually by marginalized groups aim to contest the securitizing speech of elites.

In his 2018 work, Peter de Werd undertakes an interesting attempt to combine the intuitions of the second generation Copenhagen School theorists with the practice of the military-academic environment. He employs the idea of securitization and of discursive threat construction to elaborate a new method of intelligence analysis, called Analysis by Contrasting Narratives. It represents a de-constructivist discourse analysis, which uses, as its empirical material the strategic and planning documents and the public discourse of an "enemy" in order to identify its central narratives and to understand the way that enemy defines the "threat" and the permissible limits to combat it. De Werd employs the work of Thierry Balzacq, according to whom securitization can occur not only through speech acts, but also through images, strategic documents or public policies.

De Werd's conclusion is that universities and security institutions can employ the insights of the Copenhagen school to discover the enemies' "aim" through the use of interpretative discourse analysis methods. Thus, by de-constructing the enemies' narratives, one can observe the aspects which he considers "relevant for security" and for his/her own identity.

The main criticism that can be addressed to de Werd's work is that, once we adopt an interpretative methodology and a post-positivist ontology, we can understand that both the "enemy", as well as "our team" are engaged in securitizing practices and identity narratives. These determine the very choice of the enemy and the way its reactions are understood. For example, applying this framework of analysis to the Russian-Ukrainian conflict in order to understand how and what Russia "securitizes", leads one to analyse the securitization of Russia by the West and to attempt to understand the "othering" and "orientalist" discourses that Western countries employed about Russia.

Conclusions

The article aimed to show that the erroneous understanding of the Copenhagen School in the Romanian military-academic environment relies on the simplistic and partial reading of the first book of its theorists – Buzan's *People, States and Fear*. The theory of securitization, which represents the main axis of this school of thought,

is thus excluded. It proposes a very different understanding of the ontology of security, showing that this is produced inter-subjectively through a "securitizing move" (a speech act) followed by its acceptance by the audience. Thus, the relevant difference between the theorists of the Copenhagen school and other authors is the rejection of positivist ontology and the adoption of a critical-constructivist one.

Furthermore, the article argued the second generation securitization theorists expanded the initial theory to include the concept of the audience, the idea of context and the possibility of securitization through images and public policies, without audience agreement. Finally, the article showed that the insights of the Copenhagen school are of relatively little use in the academic-military environment given that their main policy implication is that a wide debate is necessary which involves enlarging, as much as possible, the number of actors contributing to the debate. Conversely, the Copenhagen school is much more easily translatable to and useful for policy-makers. The paper also analysed an attempt to include the intuitions of the Copenhagen school in intelligence analysis. Although it does have its merits, its chances of success are limited, given the subversive nature of this framework of analysis.

References:

1. Aradau, C. (2004) "Security and the democratic scene: desecuritization and emancipation", *Journal of International Relations and Development* 7 (4): 388-413.
2. Aradau, C. (2008) *Rethinking Trafficking in Women: Politics out of Security*, Palgrave MacMillan.
3. Aradau, C. (2010). "Security That Matters: Critical Infrastructure and Objects of Protection". *Security Dialogue*, 41(5), 491-514.
4. Aradau, C. (2015) "Security as universality? The Roma contesting security in Europe". In Thierry Balzacq.ed. *Contesting security: strategies and logics* Routledge:101-115.
5. Balzacq, T (2011) "A theory of securitization: Origins, core assumptions, and variants" in Thierry Balzacq (ed.) *Securitization Theory: How Security Problems Emerge and Dissolve*, London: Routledge: 1-31.

6. Balzacq, T. (2005). "The Three Faces of Securitization: Political Agency, Audience and Context". *European Journal of International Relations*, 11(2), 171–201.
7. Balzacq, T. (2008) "The policy tools of securitization: Information exchange, EU foreign and interior policies". *JCMS: Journal of Common Market Studies*, 46.1., 75-100.
8. Buzan B, and Wæver, O (1997), "Slippery? Contradictory? Sociologically unstable? The Copenhagen school replies", in *Review of International Studies* 23(2):143-52.
9. Buzan, B, de Wilde, J și Wæver, O (1998) *Security: A New Framework for Analysis*, Boulder CO: Lynne Rienner 1998.
10. Buzan, B. (1983) *People, States and Fear: The National Security Problem in International Relations*, Harvester Wheatsheaf.
11. Côté, Adam (2016), "Agents without agency: Assessing the role of the audience in securitization theory" *Security Dialogue*, 47(6):541 – 558.
12. De Werd, P (2018) "Critical Intelligence Studies? A Contribution" ISA ISS 2018 Conference Draft.
13. Diesen, G (2015), *EU and NATO Relations with Russia: After the Collapse of the Soviet Union*, Ashgate Publishing, Ltd.
14. Floyd, R (2007) "Towards a consequentialist evaluation of security: bringing together the Copenhagen and the Welsh Schools of security studies" *Review of International Studies* 33 (2): 327-350.
15. Floyd, R (2010), *Security and the Environment: Securitisation theory and US environmental security policy*, Cambridge: Cambridge University Press.
16. Floyd, R (2011) "Can securitization theory be used in normative analysis? Towards a just securitization theory" *Security Dialogue* 42 (4-5): 427-439.
17. Floyd, R (2015) "Just and unjust desecuritization" in T Balzacq (ed.), *Contesting Security: Strategies and Logics*, London and New York: Routledge, 122-138.
18. Hansen, L. (2011). "Theorizing the image for Security Studies: Visual securitization and the Muhammad Cartoon Crisis". *European Journal of International Relations*, 17(1), 51–74.
19. Katzenstein, Peter J. (ed.) (1996) *The Culture of National Security: Norms and Identity in World Politics*, New York: Columbia University Press.
20. McDonald, M. (2008). "Securitization and the Construction of Security". *European Journal of International Relations*, 14(4), 563–587.
21. McSweeney, B (1996) "Identity and security: Buzan and the Copenhagen school", in *Review of International Studies* 22(1): 81-94.

22. McSweeney, B (1998), "Durkheim and the Copenhagen school: a response to Buzan and Wæver", in *Review of International Studies* 24 (1):137-140.
23. Mészáros, E.L. (2017) *Dimensiunea de securitate ca declansator si rezultat al modificarii frontierelor Uniunii Europene*, Tritonic: București.
24. Roe, P. (2008). "Actor, Audience(s) and Emergency Measures: Securitization and the UK's Decision to Invade Iraq" *Security Dialogue*, 39(6), 615–635.
25. Roe, P. (2012) "Is securitization a 'negative' concept? Revisiting the normative debate over normal versus extraordinary politics". *Security Dialogue*, 43.3., 249-266.
26. Stritzel, H. (2007). "Towards a Theory of Securitization: Copenhagen and Beyond". *European Journal of International Relations*, 13(3), 357–383.
27. Taureck, R (2006) "Securitization theory and securitization studies" *Journal of International Relations and Development* 9 (1): 53-61.
28. Wæver, O (1989) *Security, the Speech Act Analysing the Politics of a Word*, Paper presented at the Research Training Seminar, Sostrup Manor, June 1989, Revised Jerusalem/Tel Aviv June 25-26, 1989, https://www.academia.edu/2237994/Security_the_Speech_Act_-_working_paper_1989.
29. Wæver, O (1995) "Securitization and desecuritization", in Ronnie D. Lipschutz (ed.) *On Security* (New York: Columbia University Press), pp. 46–86 reproduced in Hughes, C.W and Lai Yew Meng (eds.) (2011) *Security Studies: A reader*, London and New York: Routledge.
30. Wæver, O (1998b) 'Security, Insecurity and Asecurity in the West-European Non-War.
31. Wæver, O (2003), *Securitisatio: Taking stock of a research programme in Security Studies*, <https://docplayer.net/62037981-Securitisatio-taking-stock-of-a-research-programme-in-security-studies.html>
32. Wæver, O (2011) "Politics, security, theory", *Security Dialogue* 42 (4-5): 465–480.
33. Wæver, O, Buzan, B de Wilde, J. (1998) *Security: A New Framework for Analysis*, London and Boulder, Co: Lynne Rienner.
34. Wæver, O, Buzan, B Kelstrup, M, Lemaitre, P (1993) *Identity, Migration and the New Security Agenda in Europe*, London: Pinter Publishers.
35. Wæver, O. (1999). "Securitizing Sectors? Reply to Eriksson". *Cooperation and Conflict*, 34(3), 334–340.
36. Wendt, Alexander (1999), *Social Theory of International Politics*, Cambridge: Cambridge University Press.
37. Williams, M. (2003), "Words, Images, Enemies: Securitization and International Politics" in *International Studies Quarterly*, 47 (4): 511–531.

A CALL TO ACTION: RESPONDING TO RUSSIAN HYBRID WARFARE

Caroline GRACE*
Jiaming HUANG*
James M. KEAGLE*

Abstract

Using its well developed and practiced programs in propaganda, deception and denial, Russia has conducted its hybrid warfare and anti-access area denial strategy using the 21st century information technologies of communication. In light of Russia's annexation of Crimea, Romania felt threatened by Russia's use of information campaign, especially the narratives that seem to have polarized the Romanian society and discredited the NATO establishment from its prompt execution of its Article 5 commitment. Confronted with these threats, Romania and NATO must understand war in the hybrid domain on an aggregate and its effect on Romania in particular.

Keywords: *hybrid warfare, Russia, propaganda, disinformation.*

Introduction

The concept of hybrid warfare is not new. It has been the standard practice of the Soviet Union in the past to make use of subversive measures to gain influence and shape the political climate in Europe. The current tactic that the Russian Federation has in part adopted today is fully consistent with its long developed history of deception, disinformation and denial (*maskirovka*). In a testimony before the House Committee on Armed Services on March 22 2017, Christopher S. Chivvis from the RAND Corporation defined 21st century "hybrid tactic" as Moscow's use of subversive non-military instrument

* National Defence University, USA.

* National Defence University, USA.

* Professor at National Defence University, USA.

to divide and weaken NATO, subvert pro-Western governments, and polarize Western societies. More generally, one can define the measure of an “information campaign” as providing intentionally false and disseminated messaging, or in other cases, deluding facts or defying objective truth (Chivvis March 22, 2017). Although the concept of hybrid war is not necessarily new, the tactics Russia adopts today are not identical with those implemented during the Cold War and earlier in the 20th century. Moscow is less bound to ideology, which has not been the case previously. Sometimes referred to as the Gerasimov Doctrine, named as such after General Valery Gerasimov’s 2013 article, “The Value of Science is in the Foresight ...,” this has been the subject of detailed discussion throughout the security community (see, for example, Fedyk, 2016).

The frequent use of social media and cyber operations is also relatively new and can be very difficult to counteract. Most recently, tension has risen between Russia and Romania in the aftermath of the latter’s reaffirmation of its NATO commitment. While Romania sets its agenda in close cooperation with the security policies of the Euro-Atlantic community, many within Romania remain sympathetic to its historic ties to the Soviet Union and the Warsaw Pact. In light of these rising domestic tensions, some believe Romania was and still is vulnerable to the Kremlin’s disinformation and misinformation campaigns. This paper will explore the Russian information operations campaign against NATO, specifically against the U.S. and Romania, and its tactics and implications. It concludes with a set of recommended NATO responses.

Russian Information Campaign in the United States (and beyond)

Russia’s information campaign extends further than asserting its influence in the Black Sea region. The United States fell victim to Russian hybrid war as well, namely in the 2016 Presidential election. In 2018, Special Counsel Robert Mueller indicted 12 Russian military personnel for felonies of “interfering with the 2016 U.S. presidential election” by engaging in cyber operations that “involved the staged

release of documents stolen through computer intrusions” (Robert S. Mueller 2018).

The indictment provided an in-depth overview of how the Main Intelligence Directorate of the General Staff (GRU hereinafter), Russia’s military intelligence agency, operated to meddle with the U.S election. Subsequent reporting from the U.S. intelligence community outlined similar operations in the 2018 elections.

The process is really quite simple: either by spoofing or spear phishing, or both. The former refers to the act of a cybercriminal to create a fictitious sender address for an inbound email in order to mislead the recipient of this email into believing that it was sent from a reliable and trusted ally. The latter refers to the exercise of cyber-crime by use of email targeting a specific recipient or a chosen group of recipients who are usually administrators of the victim organization.

A spear phishing email appears as a note from a trusted colleague. The recipient will see that it was sent from a recognized home address, but in reality it was sent by cybercriminals who are targeting confidential information. The content of these emails typically contains a security notification instructing the user to change their passwords by clicking on an embedded link. These links would bring the victim to a website or IP address created by the GRU or another intelligence entity. If the victim chooses to access their websites, the hackers can then install a program that allows them to monitor the victim’s computer screen. Once the aggressors gain access to monitoring the computer screen, they will steal passwords and obtain access to the organization’s network which, in its turn, enables access to the organization’s finances, funding, opposition research, and campaigning plans (Robert S. Mueller 2018).

Similar instances also occurred in other NATO States. Russia has made it very clear how it feels about pro-Western nations. They are seen as threats. The Kremlin took an interest in Montenegro as well. Russia responded with an information campaign attack funded by Russian oligarchs to oppose Montenegro’s NATO membership and subsidizing small anti-NATO memberships and pro-Russian political parties in the country. Russian efforts were made to polarize and decouple opinions in the country to undermine Article 5, i.e. the

collective defence clause, of the North Atlantic Treaty Organization. The Kremlin tried to subtly interfere at first; however, when that proved ineffective, it moved on to a more aggressive approach and carried out an armed *coup d'état*. The use of pan-Slavic nationalism and domestic polarization has also led to the “intrusion” in Crimea, providing seemingly sound ground for invasion. In fact, Russian Chief of the General Staff Gerasimov wrote in February 2013 about this, coining the concept of “hybrid war” by pointing to the colour revolutions as part of a deliberate Western strategy. This article first appeared in the *Military-Industrial Kurier*, and has become the point of reference for Russian hybrid tactics, centralized and organized in a collective effort fuelled by what has commonly been referred to as the “Gerasimov doctrine” (Bartles 2018). Earlier Russian attacks in Estonia (2007) and Georgia (2008) seem to fit nicely in this pattern.

The Nature of Romania’s NATO Admission and its Commitment to the West

Romania’s shift and later its commitment to NATO and the EU were evidently centred on a desire to secure its national interest and protect it from Russia. Since 1990, the nature of Romania’s expectation for joining both NATO and the EU was directly connected with its concern for security, and to a lesser degree, economic growth.

Romania’s relations with NATO started a few months after the 1989 Revolution. Despite being one of NATO’s newer clients, Romania was the first post-communist country to join NATO’s Partnership for Peace program. When the Romanian Prime Minister, Petre Roman, came to visit the NATO Headquarters in October 1990 (Ministry of Foreign Affairs n.d.), Romania had been embroiled in what is now known as the Black March, a series of inter-ethnic clashes between Hungarians and Romanians in Targu Mures, Transylvania, in March 1990. It was also concerned with emerging bonds between Bulgaria and Russia in part a result of energy dependency and religious ties. The former Yugoslav crisis in 1991 was likewise a threat to Romania’s national security. Confronted with these challenges to territorial integrity and sovereignty, Bucharest’s friendliness towards NATO was, from very early on, strategic and comprehensible given its eminent

need for security. These conditions, encompassed by the Russian Federation's interest in incorporating Southern Slavs into its declined population and Romania's own incompetence to surmount Russian political influence, at last compelled Bucharest to join NATO and the Atlantic Spirit in search for a long term security insurance (Cosmin Florian OLARIU, Daniel GHIBA 2018).

Romania's relationship with the EU served the country's own national interest as well. Romania's normalization of the relations and engagement with the European Union began simultaneously with its effort to become a potential NATO member. Romania's tilt to the West was established when it signed *The Accord of Association of Romania to the European Union* in 1995, but one could argue that the real progress began as early as 1974, when the nation became a beneficiary country of the European Union *Generalized System of Preferences* (Ministry of Foreign Affairs n.d.). In the beginning of this process, Romania's interest to join the European community was largely driven by economic and political needs. It was the EU member status, for example, that contributed significantly to a favourable settlement on the dispute of Maritime Delimitation in the Black Sea on the UN International Court of Justice (from Romania's perspective). After the collapse of the Soviet Union, Romania struggled with several financial crises and suffered from its lack of expertise in managing fiscal and monetary policies. Despite Bucharest's will to reform its economy, Romania's national resource fell short of expectation, driving the nation's decision makers again in search for external support (Cosmin Florian OLARIU, Daniel GHIBA 2018).

Although the European Union didn't offer much in terms of security assurances, Romania believed accession to the Union would increase its importance in NATO. In addition, the appearance and manifestation of multinational organized crime and other new unconventional threats challenged Romania's economy as well as its security. Following the collapse of the Soviet Union, Romania faced unprecedented non-state threats and alarming financial difficulties. Given these circumstances, one can assume a sense of reciprocity in the nature of Romania's commitment to both NATO and the EU. On the one hand, Bucharest can partially outsource its defence policy to a reliable

partner. On the other hand, it must provide its partners with offensive military bases to withhold access to the Black Sea in an effort to contain the Russian Federation.

Since 1991, Romania's path to becoming a NATO and EU member state was long and burdensome. However, our country was able to demonstrate a clear commitment to collective security and NATO, especially to the United States, via its participation in the international engagements in both Iraq and Afghanistan. In a 2003 Helsinki Commission Briefing on Romania's status moving towards NATO and the EU, it was evident that Romania's support for the Western military action in Afghanistan, Iraq, and Kosovo had created the impetus within Romania for its drive for NATO membership. The U.S., on the other hand, would gain a loyal ally and partner next to the Black Sea (in addition to the increasingly problematic Turkey). This bilateral relation and U.S. support were necessary conditions for Romania to enter both NATO and the EU. While language, culture, and history all played against Bucharest's decision to join the West, it was the participation of the Romanian Armed Forces in the Balkans, Afghanistan, and Iraq that secured NATO accession and admission to West's most powerful collective security alliance (March 29, 2004).

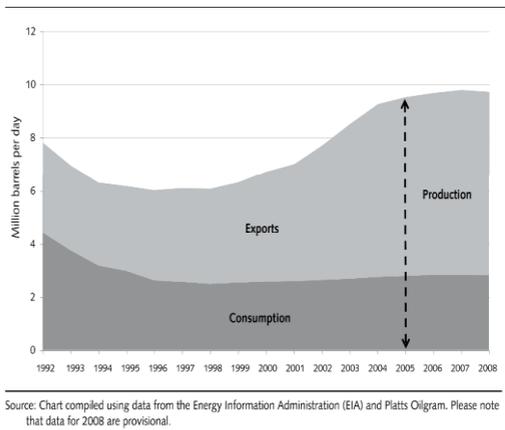
In 2005, Bucharest signed the "Access Agreement" with Washington (Ministry of Foreign Affairs n.d.), which codified the presence of U.S. troops on Romanian soil. Romania hosted multiple NATO training facilities and was home to several American "lily pad" bases. After its admission to NATO, Romania maintained a sturdy and growing level of commitment. Mihail Kogalniceanu (MK hereinafter) and Constanta Air Base in Romania, for example, have become NATO's key hubs for logistics support to Afghanistan. Construction for Aegis BMD ashore at Deveselu began in 2013 as part of Phas 2 of the European Phased Adaptive Approach. Missiles became operational in 2017. The same year, Cincu, Romania, became home to NATO's Joint National Training Centre.

Russia's Reaction

Romania's full embrace of NATO triggered an almost immediate Russian response. Evidence suggests that NATO's decision to deploy the

new Aegis ashore ballistic missile defence system (State September 13, 2011) in Romania's recently established Air Base at Deveselu inspired hostile Russian reactions. Former U.S. Assistant Secretary of State, Frank Rose stated that the deployment carried no intentional purpose of "undermining Russia's strategic deterrence capacity". However, Moscow worried that this movement would damage its nuclear deterrent capability. In addition, Russia's envoy to NATO, Alexander Grushko, asserted that by deploying the MK-41 vertical launch system in Deveselu, the U.S. has violated the bilateral agreement under the Intermediate-Range Nuclear Force Treaty. From this point of view, the U.S.'s recent threat to withdraw from the INF Treaty itself will almost inevitably reinforce Russia's existing belief that it has been the target of recent NATO deployments in Romania. To Russia, it is part of a pattern that began with the Partnership for Peace and has advanced NATO into the territory of the former Warsaw Pact, and the former Soviet Union itself. NATO commitments reached in London (2012), Chicago (2014) and Warsaw (2014) regarding deterrence, assurance and forward deployments strengthened Russian fears. They likely sparked Novorossiia claims, hybrid warfare in Ukraine/Crimea, and the social media onslaught to message the people in Russia's near abroad to re-think their Western orientation and re-join Mother Moscow. The West and Russia now seem fully captured in an action-reaction escalatory spiral.

Russia's reaction has also played out in the world and regional energy markets. The Black Sea is a vital hub for transporting Russian oil and natural gas to Europe. NATO "control" over this area could further amplify Russia's concern about its energy dominance that is also threatened by the America-led hydrofracturing revolution and the influx of LND to Europe and the regional and world energy markets.



The Russian oil and gas sector inherited the drilling technology and considerable wealth from the Soviet Union. Privatization of the oil sector after the collapse of the Soviet Union brought Russia access to foreign markets. A new Russian policy inclined to maximize profit, rather than to reinforce domestic consumption, allowed most of the incremental oil to be exported.

Figure 1: Russian Balance, 1992-2008

The Russian Oil industry also inherited one other thing from the Soviet Union – a good stabilization policy. Russia asserts a strong hand in the Middle East and Central Asia from time to time, but rarely has it employed oil as a political tool in its dealings with customers in the west. This stability of the supply chain that Russia was able to ensure offered its clients in Europe reliability, security, and diversity in the oil industry, differentiating Russia from other OPEC suppliers, and giving Russia enormous competitive leverage against oil suppliers from the Middle East. As Russian President Vladimir Putin has nicely put it, “the role of [Russia] on international energy markets determines, in many ways, [Russia’s] geopolitical influence.” To put it differently and in a way in which President Putin will be reluctant to express publicly, Russia is heavily dependent on its oil and gas revenues. Without further diversifying its economy, Russia simply could not contemplate any action that might destabilize its export of crude oil, petroleum products, and natural gas to Europe (Ebel July 2009). But all that changed with its policies toward Ukraine in 2014 – and even sanctions have not caused Russia to reverse course. As the Nord Stream pipelines with Germany suggest, a mutual vulnerability exists between suppliers and consumers.

Thus, the Russian economy resides on the thin end of the wedge. On the one hand, the income from exporting oil and natural gas makes up a majority of Russia’s fiscal revenues. On the other hand, Russia’s

dependency on exportation of oil makes its foreign and domestic policy revolve around producing and transporting oil products.



Source: U.S. Central Intelligence Agency (unclassified).

Figure 2: Competing pipelines in the Southern Corridor for Eurasian Gas Exports to Europe

Russia has two ways of shipping Crude Oil, petroleum products, and natural gas, either by loading oil in LNG and loading them on tankers or by pipelines. In general, tankers are preferred because of the high cost of building infrastructure for pipelines and, in Russia's case, because the transmission of the nation's oil and gas exports will have to go through the Black Sea (unless and until climate change truly becomes a game changer for world energy transport through the Arctic and the Northern Route). Therefore, deployment of land-based SM-3 interceptor ballistic missile defence system at Deveselu Air Base beginning with that in September 2011 could be seen by Russia as a demonstration of NATO's capability, in an expansionist scenario, to disrupt Europe's access to Russian oil and natural gas exports (Ebel July 2009)—as well as precursors to an invasion.

Although the development of NATO's missile interception capability in Romania was defensive in nature, and was in close coordination with Romania's request for a long run security guarantee, tension between Russia and NATO allies in Eastern Europe, namely Romania, has intensified in the immediate aftermath of Romania's increasing involvement in NATO's collective defence. In fact, the Russian Federation has specifically listed Romania as part of its security threat as early as 2014, when it addressed the Ballistic Missile Defence elements in Romania as potentially threatening to Russia's security (*Russian Military Doctrine* (Cucuş, 2015)). Most importantly, there is a possibility that Romania's reaffirmed NATO commitment will incentivize Russia to adopt hybrid measures, like its unilateral annexation of Crimea, by financing anti-Semitic political parties, by corrupting and exploiting Romanian public media, or by other measures supported by an aggressive propaganda machine supervised by a rogue state. Russia could even have leveraged its activities in Romania through pressure in neighbouring Moldova and its breakaway sector, Transnistria. Although what happened in Ukraine could not have invoked Article 5 of the NATO Treaty, to which an organized collective response could have been activated, Romania, Poland, and other Baltic and central European states will continue to urge NATO to play a more preventive and active role in maintaining the common defence. NATO needs to develop its own methods capable of effectively responding to new security threats represented by hybrid war, information operations, and others alike. In order to ensure common defence, NATO must understand the nature of Russian hybrid tactics and information operations, and, if needed, fight a preventative war in the same hybrid domain (CUCUŞ 2015).

Russian Hybrid Warfare in Romania

Romania's participation in NATO and the EU provides a level of consistency between Bucharest's foreign policy and that of its Western partners, which, as previously noted, collides with Russia's strategic interest in the Black Sea and Eastern Europe. As a result, Romania has been a target of Moscow's information operations in its continued effort to polarize societies, change popular attitudes, and prepare the ground

for unilateral occupation. As a member of NATO, Romania should not feel threatened by a designated military aggression from any State, per Article V assurances. However, the approach from a so-called “hybrid tactic,” where social phenomena and public opinion are directed to further polarize the State, puts Romania literally on the front line and forces both Romania and NATO to prepare for a good fight for the high-ground in a hybrid war.

In Romania, the language barrier impedes the precise retransmission of political messages. However, existing religious, cultural, and historical ties can still encourage pro-Kremlin sentiment, defy objective truth, and provide grounds for incorrect information to grow. Romanian society came under strong Soviet influence during the Cold War. Besides political and economic interconnectedness, socio-cultural institutions built by the Soviet Union were also closely adhered to by Romania authorities. After the collapse of the Soviet Union, Moscow’s political and economic leverage shrank, but the strong cultural, societal, and educational ties with Russia remained at the heart of the older generations of Romanians. Romania also has a strong religious tie with Russia. Its spiritual demographics are strongly shaped by Eastern Orthodox Christianity. All of these historical aspects make Russian’s information campaign in Romania a subtle case study.

In Eastern Europe, the standard practice of Russian information tactic has been centred on appealing to and messaging with ultra-nationalistic political views and ethnic loyalties. Pan-Slavic themes and the emphasis of Russian minorities abroad have been the main media upon which pro-Kremlin sentiments lean and inspire. Romania is unique in Eastern Europe in this regard. Pan-Slavic sentiment does not resonate because Romanians are of Latin descent. There is only a small number of ethnic Russians, not enough to form a considerable political group either. Even with these difficulties, the Russian information campaign has achieved some successes and proved yet again the effectiveness and coerciveness of its hybrid tactics. Recent polling results speak powerfully: Romanian public trust in the European Union fell 24% from 2004 to 2017. The same poll also revealed a relatively low social trust in the U.S. for two consecutive years stagnating at roughly 30% (Cosmin Florian OLARIU, Daniel GHIBA 2018). While it is

beyond the scope of this paper to draw a definite conclusion from these data, it seems beyond coincidental that this change occurred at the same time as the implementation of Russia's hybrid campaign.

Common Audiences of Russian Information Campaign

Malign activities to improve Russia's image and spread pro-Moscow sentiment are exercised online through the creation of alternative reality, rebranding facts, and concrete arguments. In a 2017 World Press Freedom Index, the media landscape in Romania was categorized as being "manipulated and spied on." The Romanian press, as the report continues, was composed of "excessive politicization," "corrupt financing mechanism," and "infiltration of [foreign] intelligence." The Kremlin also has a large presence on social media. Figures from Romania's National Institute of Statistics show 10.6 million Romanians have access to the Internet. The rich digital landscape has allowed Russian malign activities to further cultivate confusion, undermine objective truth, and spread mistrust in Western values and solidarity.

Among the most vulnerable groups susceptible to being the subject of Russian propaganda are Romanian nationalist and right wing swingers. These groups often depict themselves as staunch, often inflexible, believers in Romania's uniqueness among nations. They castigate Romania's alliance with the West; militate for a non-aligned and independent path for the country, arguing commonly in favour of a friendly relation with Russia. The usual message conveyed is that of a bleak international milieu where the West, by and large, and American hegemony, in particular, is blamed for disguised imperialism, exploitation of world resource, incentivizing or supporting regional conflict, while having in our domestic sphere a corrupted leadership and heavily biased media.

Religious conservatives, usually ultra-orthodox Christians, have emerged as another vulnerable group as well. This group commonly draws on Romania's ethnically superior traditional society and religious beliefs to criticize the dysfunctional, decadent West.

Soviet Union sentimentalists, most of who have aged while witnessing Romania's transition from a Soviet to a Western-style

society, are also subject to the influence of Russian propaganda. This group has witnessed what they would refer to as a period of chaotic transition to the West when Romania was being economically marginalized, socially discontent, and politically vulnerable against foreign governments. However, this nostalgia for the Soviet ways is not a strong current within Romania. While it is true that Romania experienced some drop in living standards and job stability post-1989, this phenomenon had largely run its course by the end of the 1990s.

Instruments of Russian Information Operations in Romania

The ample use of social media is a common approach adopted by Russian intelligence officers. Independent news agencies, blog writers, commentators provided Kremlin with abundant room to deliver manipulative messages that required little fact-checking or journalistic deontology. Opinion pages on the Internet can also create a snowball effect on social media, allowing targeted audiences to easily fall into cognitive group bias.

Troll farms, also known as “patriotic hackers” are employed by the Kremlin to spread false and misleading information generated by Russian media outlets such as *Russia Today* and *Sputnik News*. These media outlets take cues from state-controlled agencies and spread particular narratives that the sponsor intended to circulate in the public domain. Once information is out on the Internet, intelligence officers then prey on “useful idiots” who are a part of the public but have the tendency to re-enforce pro-Russian sentiment. The Kremlin also tries to divide NATO and subvert pro-Western governments by drawing on the success from the Soviet era, or by amplifying anti-NATO rhetoric, through the use of media. These tactics try to gauge a rise in emotion by putting out old war nationalistic media to create a stronger sentiment of patriotism and nationalism, which aligns with the pro-Russian narrative.

Moscow’s hybrid war tactics are known for their diversity and specificity. The Russian disinformation campaign sometimes takes into account the character of the specific nation it targets, and then manipulates political sentiment and cultural characteristics. Russia capitalizes on Romanian cultural vulnerabilities such as the make-up of different groups in Romanian society. Russian state-sponsored agencies

have notable influence over think tanks, human rights groups, and politicians; most importantly, they from time to time have attempted to exercise “authority” over the Romanian Orthodox Church. Russia has a history of using the Orthodox Church as a propaganda tool by presenting “traditional” Russian values as being traditional Christian values. The Kremlin has the church as an ally inside Russia and thus a mass supporting audience.

However, transferring this influence tool within Romania has been problematic, as the two Churches are not well-connected. In fact the visit of Patriarch Kirill to Bucharest in October 2017 marked the first such visit since Patriarch Alexy I visited Romania in 1962.

Apart from *Sputnik* and *RT*, domestic Romanian media platform and outlets have no formal or proven ties to Russia. Yet, rarely is the Romanian press inclined to accommodate transparency in building their organizational and financial structures. Corina Rebegea, an expert at the Centre for European Policy Analysis, believes some Romanian media outlets are conducting “camouflage” actions aimed at indirectly conveying pro-Kremlin messages. She believes overt Russian propaganda would not have been perceived in a positive manner by a broader range of audience because of wide spread Russophobia existing in Romanian society, and that the Russians have colluded with other Romanian outlets to create a delusion through diversifying the provider of propaganda. In any case, the narratives these outlets have are similar, ranging from a pervasive, nationalistic, and anti-establishment (EU/NATO/US) campaign, to criticisms depicting Romania as a vassal of Western imperialism. This content often incorporates an effort to polarize Romanian society, including fierce criticism against not only Western society but capitalism and globalization on more general terms, which puts these progressive values in obvious antithesis with Romanian tradition. The tradition quoted here involves traditional and moral values as well as religious values. Recalling the close ties Russian Orthodoxy has with its foreign policy agenda, it is not difficult to realize the soft power instruments the Kremlin has adopted through the use of religion, and, for this reason, and one can equally raise suspicion about Russia’s role behind each of the religious, moral, and traditional values quoted in pro-Kremlin messages.

The Kremlin also uses conventional social media strategy to attract the middle-aged population and youth groups in Romania. Russian information operation agencies provide narratives that square with the criterion of being simultaneously divisive and popular. Nationalism has been such a recent subject and of great popularity for this specific reason. Right wingers often arise in impoverished areas as a result of poverty, and have been used to create a sour impression of NATO and anti-Western backlash. Many Romanians lack trust in democratic institutions because of the political corruption and lack of representation. This is particularly concerning on the road leading up to the 2019 Romanian presidential election. Russian information operations might have created a gap between Romanian public opinion and the political agenda, making it difficult for political parties to adequately adhere to public views.

The U.S. reaction was perhaps best captured by Assistant Secretary of State Wess Mitchell in his testimony to the Senate Foreign Relations Committee: “Within the Bureau, we recruited one of the architects of the Global Engagement Centre legislation from the staff of a member of this committee; we formed a new position – the Senior Advisor for Russian Malign Activities and Trends (or, SARMAT) – to develop cross-regional strategies across offices. EUR created a dedicated team to take the offensive in publicly exposing Russian malign activities, which since January of this year has called out the Kremlin on 112 occasions. We are now working with our ally, the UK, to form an international coalition for coordinating efforts in this field and have requested over \$380 million in security and economic assistance accounts in the President’s 2019 budget.” (Mitchell 2018)

Furthermore, Facebook Chairman and CEO Mark Zuckerberg testified to Congress on numerous occasions as to the magnitude of the problems (in the U.S.) and indicated Facebook was shutting down millions of fake accounts monthly (Zuckerberg 2018).

Evaluating the Effectiveness of Russian Information Operations

There is no way of assuring precision in the evaluation of information campaigns mainly because of the diversity of its

instruments. Are more Romanians inclined to oppose or resist NATO deployments or EU membership as a result of the Russian campaign? If so, what percentage of the Romanian population is involved? What are the reasons for their anti-establishment sentiment? How many of these reasons are incentivized by Russian information operations? Has the American political system and other political systems been destabilized? In attempting to evaluate the cause for these potential and difficult to measure effects, impartial judges must inevitably adopt a somewhat subjective point of view, bearing equal responsibility with the Russians for having potentially misinformed the audiences about what is happening in Romania and elsewhere. Nevertheless, there are facts that can guide us.

First and foremost, the Romanian media appears to be fertile ground for Russian information campaigns. Media are poorly regulated in Romania. In the absence of regulatory standards and norms for social media and online materials, there are no functional or practical laws that can effectively address Russian harmful activities. The difficulty here is that the Kremlin's hybrid tactic is diversified, involving the use of cyber operations to disinform and the use of public instruments, taking advantages of natural democratic inefficiencies to misinform. In the first situation, the information provided is purposely articulated, false and disseminated to meet certain agenda. In the second case, the information provided is partly or totally incorrect, but it may not have been falsified for a certain purpose. Currently, regulatory bodies do not exist to examine the quality and accuracy of information from online sources. Since the hybrid tactic mainly involves the use of the internet, it is practically impossible to prevent it from spreading due to:

1. the difficulty of overseeing the deontology and holding respective news agencies accountable;
2. the complexity in penalizing online publications, such as the potential violation of the freedom of press; and
3. the impracticality of identifying and counteracting all sources of the ideological "hybrid" risks.

When assessing the vulnerability and resilience to Russian information campaigns and hybrid warfare, the absence of a clear solution and the presence of barriers as identified above have made

Romania a useful case study. In the absence of a large Russian population and Pan-Slavic traditions, the patterns of Russian misinformation were limited to nationalism and religious extremism, both of which can be identified with some precision. These patterns feature an identical anti-Western narrative aimed at agitating audiences and creating a psychological state of paranoia in which the Euro-Atlantic frameworks are depicted in cynical terms and contrasted with a friendly and peaceful vision of the Russian Federation. In spite of the language barrier, outside observers can find narratives that elicit a strikingly similar line of argumentation in the Romanian digital environment.

The collusion between Russian government-sponsored information campaigns and Romanian domestic outlets is also noteworthy. There have been scenarios in which politicians or other persons of exceptional influence have mimicked the information strategies the Kremlin has adopted, especially its use of nationalism and conservative right-wing sentiment, usually for the purpose of fulfilling a political agenda otherwise disconnected with the Kremlin's view.

Recommendation on Potential Strategic Response

To deploy NATO resources to 1) counteract Russian information operations in Romania (and elsewhere) and 2) to respond either with preventative or pre-emptive strike in the hybrid domain means first and foremost to examine the effectiveness of such Russian activities, as being the subject of our discussion, in the fullness of its context. Should NATO view the hybrid tactic as a real and tangible threat, it should appoint a special counsel to investigate the input and output of Russian information campaigns, as well as the collusion between Russian and Romanian intermediaries. A first step would be to increase the funding of the SARMAT teams throughout the European and Eurasian Bureau region as Dr. Mitchell identified in his 2018 testimony.

Secondly, there is a real need to broaden the European understanding of security based on the assumption that hybrid war is changing in character and perhaps even in nature. An understanding of Russia's propaganda machine will create a renewed call to resist Russian malign activities as a key component of the security threat

environment in Europe and reassure NATO's establishment. Moreover, it is a concept that builds trust with NATO allies even if it is denied by Russia. In addition, it will most certainly incentivize European members to invest in emergent technologies for NATO due to the nature of the changing threat Russian hybrid warfare poses to domestic political infrastructures and cultures. The U.S. can exploit the potential to take action. Highlighting such policy could make the European public more aware and critical of pro-Kremlin messages and could improve NATO's credibility and support.

Lastly, NATO must confront more directly the conventional force imbalances that have tilted in Russia's favour along NATO's Eastern European border with Russia (Ochmanek and Rand Study, 2016). NATO should rebuild a credible conventional deterrence-by-denial through a cost imposition strategy (Nopens 17 June 2016). Followed by the conventional deterrence-by-denial ought to be the re-establishment of bilateral ground for political dialogue. Since the INF treaty appears all but dead, there must be a replacement of some sort to provide ground for re-establishing mechanisms capable of preventing unintended escalations to the nuclear realm. The Russian nuclear military modernization program in Kaliningrad cannot be ignored.

Conclusion

Compared to the success of the Russian hybrid tactics in Crimea, the Romanian case appears less definitive but equally disturbing, particularly if it reflects a broader pattern of Russian behaviour. To this date, there has not been any investigative effort to unveil any Russian involvement or other foreign interference comparable to the Mueller investigation that took place in the U.S., but perhaps there ought to be. The Russians indeed applied a hybrid framework in Crimea and Eastern Ukraine. However, it is important to note that they did so in combination with use of conventional/special forces – an actual traditional combat capability.

When Gerasimov wrote of using “political, economic, informational...and other non-military measures applied in coordination with the protest potential of the population,” he was referring to the new evolutions of the instruments of information to

destabilize the enemy state and to provoke regime change without the instigators admitting to any involvement. When Russia employed this method in Crimea and Eastern Ukraine, its “success” raised the stature of the “Gerasimov doctrine,” making the Russian general to be perceived as a mastermind of hybrid warfare. For him, state mobilization and the future military operational environment will witness the employment of “hybrid war” through the use of “information.”

Russia did indeed wage a hybrid war in Crimea and Eastern Ukraine, especially on attracting local support. However, one must not overlook Russia’s existing capability to mobilize and deploy conventional force on large scale, which was what ultimately made Crimea a feasible strategic option. We argue, therefore, that the “hybrid” domain is not a field so alienated from other conventional military practices. Rather, it should be seen as a three stage plan where the use of information operations came first to disinform or misinform a targeted population for the purpose of gaining public support for the Kremlin, quickly followed by the mobilization and deployment of conventional weaponry and the army without which the “hybrid” success would not have happened. We argue that this three stage plan of action codifies the Gerasimov doctrine most accurately in full consideration of his 2013 argument.

In a world increasingly sensitized to fake news, narratives and counter-narratives, it is challenging to know what to believe. But how we come to believe what we believe is a central function of political socialization and the transmission of national values and societal norms. Rest assured, Russia does have a strategy to attack these processes and structures—and it is employing it both in its near abroad and against the U.S. The power of algorithms and computer driven messaging makes the phenomenon of the confirmation bias all the more troubling—and deserving a serious response.

References:

1. Bartles, Charles K. (2018). *Getting Gerasimov Right, Military Review*. Washington DC: Center for Strategic and International Studies.
2. Chivvis, Christopher S. (March 22, 2017). "Understanding Russian "Hybrid Warfare": What Can Be Done About it." *Testimony before the U.S. House Armed Services Committee*. RAND Corporation.
3. Commission on Security and Cooperation in Europe and United States, (October 23, 2003). "Romania, Moving Toward NATO and the E.U." United States Congress Romania, Moving Toward NATO and the E.U.
4. Cucos, Cezar. (2015). "The Establishment of Nato Structures in Romania – Guarantee of Collective Security." *International Scientific Conference "Strategies XXI" 2* (International Scientific Conference "Strategies XXI" 2, (2015): 89.
5. Ebel, Robert E. (July 2009). *The Geopolitics of Russian Energy*. Center for Strategic and International Studies.
6. Ministry of Foreign Affairs, Romania. n.d. *Romania Ministry of Foreign Affairs*. Accessed October 22, 2018. <http://www.mae.ro/node/2131>.
7. Mueller, Robert S. III. (2018). *U.S Department of Justice Indictment June 16 2018*. U.S Department of Justice .
8. Nopens, Patrick. (17 June 2016). *Time to Restore Conventional Deterrence-By-Denail*. Belgium Royal Institute for International Relatio
9. Olariu, Cosmin Florian, Ghiba, Daniel, (2018). "The Security Dependency of Romania on Nato, EU and USA." *International Scientific Conference "Strategies XXI", 01/2018, Volume 2* 150-155.
10. U.S Department of State, September 13, 2011. "Ballistic Missile Defense Agreement Between the United States of America and Romania."

FAKE NEWS, ETHICS AND RESPONSIBILITY IN MEDIA REPORTING IN CASE OF SECURITY THREATS AND SENSITIVE ISSUES. AN EMPIRICAL RESEARCH OF THE PRACTITIONERS' EXPERIENCES*

Ileana-Cinziana SURDU*

Abstract

The article presents the results of an empirical research dedicated to the views that institutional communicators (spokespersons), journalists, and security studies experts hold on the phenomenon of fake news, ethics and responsibility in media reporting in case of security threats and sensitive issues. The study aims to provide a practical overview, capitalizing the on-field expertise of practitioners in security and law enforcement fields, and bridging the three perspectives into a unified approach for efficiently managing strategic communication in media reporting.

Aiming to encourage and empower spokespersons to get out of information bubbles, to critically address fake news and develop responsible and accountable communication patterns and behaviors in the relationship with their audience, a sociological field research has been undertaken at the level of three European states: Romania, Spain and Greece. The empirical process aimed to understand the phenomenon of fake news, ethics and responsibility in media reporting in case of security threats, and to identify the training needs, further necessary information and abilities of the target groups. The data were collected from the pool of spokespersons, journalists,

* Acknowledgement: This document was drafted with the financial support of the European Commission, as part of the CRESCent project ("Mind the gap in media CoveragE and Strategic communication in CasE of security Threats – the development of critical thinking and responsible reaction" - CRESCent Project 2018-1-R001-KA202-049449). The survey has been drafted and conducted within the CRESCent project with the contribution of "Rey Juan Carlos" University (Spain), Directorate for Information and Public Relations from Ministry of Internal Affairs (Romania), and Kentro Meleton Asfaleias (Greece), and has been coordinated by "Mihai Viteazul" National Intelligence Academy (Romania). The content of the present document is the exclusive responsibility of the author, and the National Agency and the European Commission are not responsible for the way that the information will be used.

* Researcher PhD, "Mihai Viteazul" National Intelligence Academy, Bucharest, Romania; email: surdu.ileana@animv.eu

practitioners, experts and other stakeholders in the field of security and law enforcement. The research was based on a triangulation process, combining quantitative and qualitative methods, and offering a practical overview on the phenomenon of fake news and ethics in media reporting, strategic communication, critical thinking, media literacy and responsible communication in case of security threats and sensitive issues.

The analysis of the processed data allows the identification of a set of good practices, schemes and strategies dedicated to institutional spokespersons, and (young) journalists in the field of security and law enforcement, and relevant stakeholders, in relation to responsible and ethical reporting. It identifies methods of increasing resilience to disinformation and other related aspects, and draws the needs for acquiring, developing and strengthening skills and key competences, in order to foster strategic communication, critical thinking, media literacy, fake news resilience, media ethics and responsible reaction. The results are suitable to be integrated into a practical overview of any type of approach for efficiently managing reporting in case of security threats and sensitive issues.

Keywords: *hybrid Media reporting, security threats, fake news, disinformation, strategic communication, critical thinking.*

Purpose and objectives

The main purpose of the analysis was to develop an empirical overview of the phenomenon of fake news, ethics and responsibility in media reporting in case of security threats and sensitive issues. The analysis aimed to:

- register behaviors related to practices, schemes and strategies of responsible and ethical communication in case of security threats and sensitive issues;
- register opinions related to identifying fake news and disinformation and connected aspects;
- identify means of resilience and protective factors in case of fake news and disinformation and connected aspects;
- identify needs for learning and training related to ethical and responsible media reporting in case of security threats and sensitive issues.

As part of the exploratory research, the empirical study addressed experts, practitioners and future practitioners in media reporting and public communication in security and law enforcement fields. This approach allowed for the collection of qualified opinions

and factual data, conferring a high value to the information collected. The research analysis may contribute in terms of responsible and ethical communication, literacy on fake news, disinformation and other related topics, themes to stress in connection to necessary skills and competences to be further developed and strengthened. The exploratory process allowed the interaction with the expertise and needs of both experienced and less experienced individuals from the target group categories within the study.

Research methodology

Methods, techniques and instruments: The research was based on an exploratory process, studying concepts, attitudes and behaviors in relation to sensitive issues for the public. The analysis sought to identify and clarify aspects connected to ethical and responsible media reporting, to ways of dealing with fake news and disinformation and related aspects, when addressing the public. The process allowed a deeper understanding of the opinions, attitudes and behaviors, and, at the same time, it outlined the needs for learning and further training of the subjects.

The exploratory research allowed:

- the (better) understanding of ethical and responsible communication strategies;
- the exploitation of opinions related to the protective factors against fake news and disinformation and other related aspects;
- the identification of the needs for acquiring, developing and strengthening skills and key competences related to ethical and responsible media reporting in case of security threats and sensitive issues.

The exploratory research was implemented through an empirical process, which assumes the direct observation of the reality, by collecting data through a sociological investigation. The empirical study was developed through a process of triangulation, applying both quantitative and qualitative methods. This strategy allowed both the collection of data from a higher number of respondents and the introduction of questions in the semi-structured interview guide, which

targeted the explanation of un-detailed answers marked in the questionnaire.

The study followed the configuration below:

- the quantitative method: self-applied questionnaire (on paper/computer assisted web interview);
- the qualitative method: individual interview based on a semi-structured interview guide.

The quantitative approach allowed the identification of themes and concepts, strategies and schemes related to ethical and responsible media and public communication. At the same time, the qualitative one allowed the clarification of concepts, the description of the schemes and strategies, and a correct conversion from theory to practice.

The data has been collected throughout 2019, from March to August.

Target group: The analysis relied on the on-field experiences, best practices and current workflows of institutional spokespersons, (young) journalists, and security studies experts, bridging the three perspectives into a unified approach for efficiently managing strategic communication in security and law enforcement fields.

The questionnaire has been answered by 127 respondents, out of which 90 from Romania, 8 from Greece and 29 from Spain. Out of the total respondents, 39 are women and 88 are men. A third of the sample (44 respondents) have declared that they have between 11 and 20 years of experience in the field, 22 are working in the field for less than a year and only 7 have a 21 to 30 years of experience. Most of the respondents with 11 to 30 years of experience in the field are institutional spokespersons and journalists. Respondents with lower than 6 years of experience in the field can be found in each of the professional categories targeted in the study. The interviews have been conducted with 28 experts in security and law enforcement fields from Spain (10), Greece (10) and Romania (8).

Results of the research

In order to understand the responses of the participants to the study, they have first been asked about **the significance of a “security**

threat” or a “sensitive issue” in relation to their fields of work. In case of the participants from the public relations field, a security threat is considered through the impact of the message over the public, which “is likely to create fear of panic among the population”, or which can “generate vulnerabilities for the institution’s image”. It may be caused by false, “incomplete”, or “distorted” information, or by a “lack of a firm and complete institutional point of view”. The participants who work on field interventions consider threatening a situation where a mission is faulty, or where there is a leak in the system and an employee proceeds to “declaring, violating, as well as offering personal information, or transmitting unpublicized information”. The presence of harmful actions are also mentioned as security threats, like “terrorism, nuclear energy and soft targets”, or like “those that endanger the existence of the state, for example corruption”. As a general remark, security threats or sensitive issues are considered to be any situations that endanger the individuals or the society as a whole.

Radicalization or extremist messages are seen as negative actions towards the constitutional structure of the societies, which lead to the increase of hatred and the rejection of diversity. Also, the participants evaluate that it is difficult for the population to identify terrorist communication, as the society does not think of habitual ways in the possibilities of a terrorist attack.

*“So, I think as far as they are trying to destroy our way of life, they are trying to destroy the constitutional structure of our societies.”
(Academia)*

“I think that it is almost impossible to distinguish terrorism from communication. It is in the roots of terrorism to spread threat and to challenge the society. I would say that probably in the last two decades there have been more successful use of communication and they have realized that they cannot really win.” (Academia)

For the respondents to the questionnaire (N=127), a **successful message** includes clear information (88, 10%), true data (73, 80%), and brevity (46, 80%).

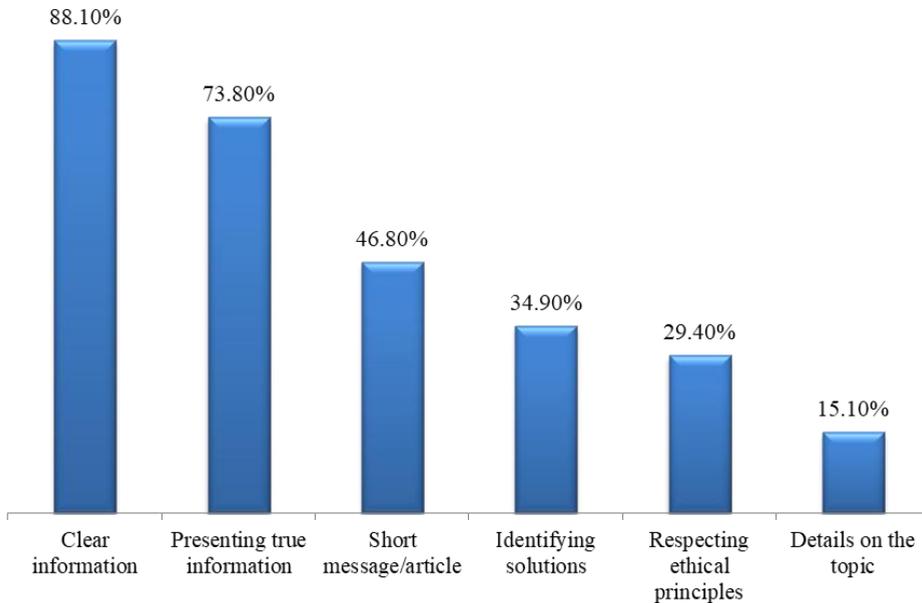


Figure 1: Indicators for a successful message (Source: the author)

A successful message is seen as one that reaches the target audience, and which the target audience receives as intended. A successful message must be clear, “with noise” and “interesting for the people”. It also has to be adequate and offered at the right moment. In the case of media, a message is considered effective when it is published in the main newspapers, so it is validated by the professionals. The social networks are a more difficult to monitor channel, though. In case of the general public, the impact could be monitored through the social media channels, while at political level, a successful message will create awareness among politicians so they would act or comment about the issue.

“A successful, effective message is one that achieves the effect that the issuer thought it will have.” (Academia)

*“From our point of view, a successful message is one that fulfills the function we had previously thought for that message. The fundamental thing is to tell what it is of interest for the people.”
(Institutional spokesperson)*

*“In the 21st century, when you have a lot of impact in social media, you can say that your message has reached the public. Even if it’s a negative reaction, if people are talking about it, it means that your message has reached the general public. If the rest of the main news outlets in that country pick up the story, we consider it a success.”
(Journalist)*

The success of the message is also connected to its purpose. For instance, an informative one contains explanatory text accompanied by a link or a video; an inspirational message contains a short text and puts great focus on the visual (photo, graphic or video); in case of the news and updates, it should contain a very short text with a link to the news article.

The main risks when reporting on security threats or sensitive issues are considered to be the possibility of being misunderstood (N=127) (76, 4%), of transferring panic to the public (70, 1%), and the generalization of the issue (53, 5%).

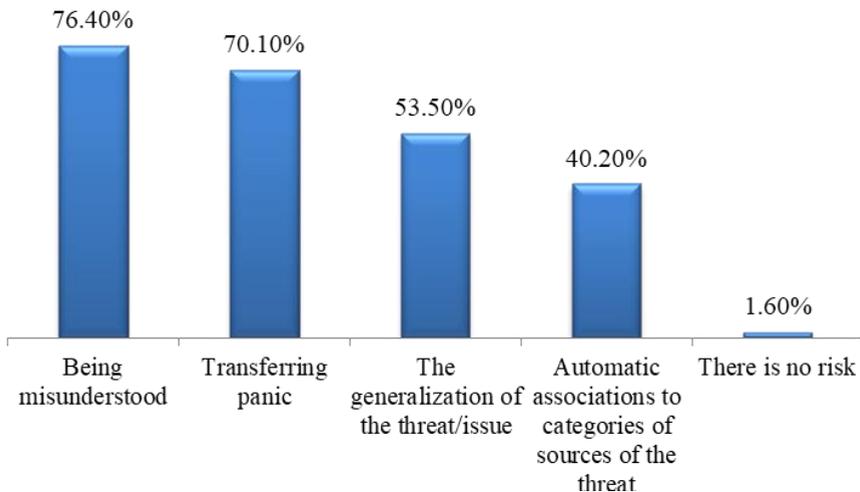


Figure 2: The main risks when reporting on security threats or sensitive issues (Source: the author)

In order **to ensure a positive response** from the public when communicating on security threats or sensitive issues, the participants to the study highlighted a series of strategies/solutions they apply or recommend. **These strategies focus on three aspects: 1) the content/form of the message, 2) the action of reporting and 3) the intervention itself.** In what concerns **the message**, it has to be clear, “short, concise, and to ensure that the situation is under control”, “easy to understand” and it has to present “real and verified data”. The communication must present the solutions to the problem, as well as the preventive and counteraction measures that are being undertaken. **The action of reporting** should be prompt, ongoing during the development of a certain situation, “early, which is before accumulating fears”. It is also highlighted that it is important to communicate “with compassion the information with impact over the communities or families”. “Correct selection of the information that are of interest for stakeholders, verifying the information before publishing it and communicating continuously with the press institutions, the opinion makers, the online environment and the social networks”, “the communication of clear and true information directly to the target group through the own web pages or through socializing networks”, or “the dissemination of the institutional message by the opinion makers outside the institution” are actions to be taken into consideration when reporting. Besides the content and the form of the message and the ways of addressing to the public, it is important also to focus on presenting **the intervention** itself, by communicating “about the undertaken actions”, taking into consideration “the equilibrium between the needs of the public for immediate and complete information, and the need of the institution to ensure the confidentiality of specific situations established by the law”. On the other hand, other participants suggested that a positive response is dependent on “giving only the main information, without details which could put in danger the problem solving by the authorities, ensuring the safety of the citizens in the same time”. It is also mentioned the importance of measuring the impact of the message over the public.

"We seek that the message is not flat, only with text, and it contains visual data. For this, we use emoticons, dots etc." (Institutional spokesperson)

"I think that the role of media is to create confidence." (Academia)

Among the **factors that determine the efficiency** of the communication/reporting activity are considered to be the use of images, the short reaction time, the validity of the information, the credibility of the communicator, using efficient channels of communication, but also characteristics of the content already mentioned above – clarity, shortness, transparency, ease of understanding, presenting interesting aspects etc. In what concerns the communicators, the participants evaluate that they "have to know very well the field of activity, to have the capacity to elaborate complete and pertinent point of views and to always find solutions"; other important factors highlighted are "the level of training of the spokespersons, how well they know the procedures and the way of intervention of their own structures, the intervention technique, the specific legislation, the way they communicate with the logistic support they benefit of", but also "the relationship they have with the mass-media representatives". Technical language is to be avoided, and also the references to the institution or job titles. Not including personal opinions and presenting only facts may lead to the efficiency of the message. The public is an element to be taken into consideration when reporting; the message can reach the targeted response also if it is designed based on the characteristics of the audience.

"We try to make reports without including personal opinions. We only write facts. We leave the opinions for the newspapers, or the television, so our main aim is giving the information as quickly as possible, and trying not to do any mistake." (Journalist)

A **message can fail** "when a piece of information is missing", or "when someone chooses an irrelevant part of the message you are

trying to provide the society with.” Also, if the information is not adjusted, or if it is not offered at the right time, or it contains technical perspectives, it can lead to a failure in terms of communication. If the message does not reach the public, it may also lead to the loss of trust in the respective news media. Also, a message is prone to fail if it involves political or economic motivation for dissemination. Elements like noise, semantics, or cognitive dissonance are to be taken into consideration as signs of a failed message.

Twenty-five of the respondents to the questionnaire declared that they have faced the situation of reporting on a security threat or a sensitive issue which has been discussed by the public in a different way than presented, so it created confusion, misunderstanding or panic. In such cases, they proceeded to further explanations, “by using a simple language”, “with arguments and pertinent solutions”, but also to finding institutional partners who wanted to disseminate the message, and establishing a “permanent dialogue with the mass-media representatives to clear the unclear aspects”.

A negative response from the public may occur, according to the participants to the study, as a result of delays in communicating, the use of general descriptions, not using the principle of “a unique voice”, not using verified data, or the use of “an aggressive style to attract attention (which determines the loss of trust)”. Among the factors that enable or allow the dissemination of faulty messages on a large scale, there were mentioned the internet itself and the socializing platforms as propagation channels, from the perspective of “the huge speed of the communication flow” and the possibility of circulating fake news, “the thirst of celebrity” of the communicators, the lack of reaction, or the lack of training of the communicators.

When talking about the discrepancies between social reality and messages received by the public, the majority of respondents to the questionnaire (103 out of 127) evaluated as a main cause the “creative” media coverage that is balancing between obtaining profit and respecting ethical standards of reporting.

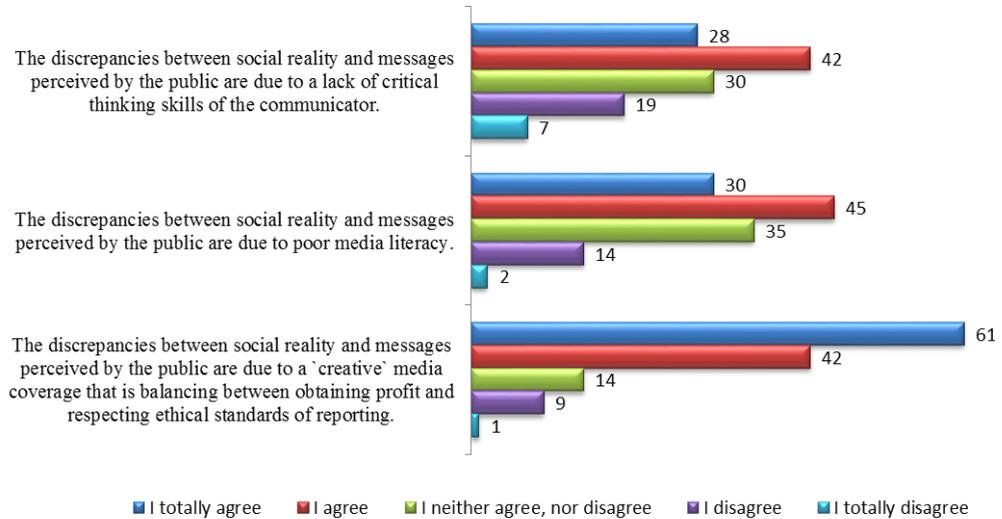


Figure 3: The factors that enable or allow the dissemination of faulty messages on a large scale (Source: the author)

In order to **reduce the spread of harmful actions** to the public, the respondents to the questionnaire consider that the communicators and the media should allocate the necessary time to understand what it is happening (75, 90%, N=108), should contribute to the raising of awareness among the public (68, 50%, N=108), or should contribute to the building or the reestablishment of trust in national institutions (56, 50%, N=108).

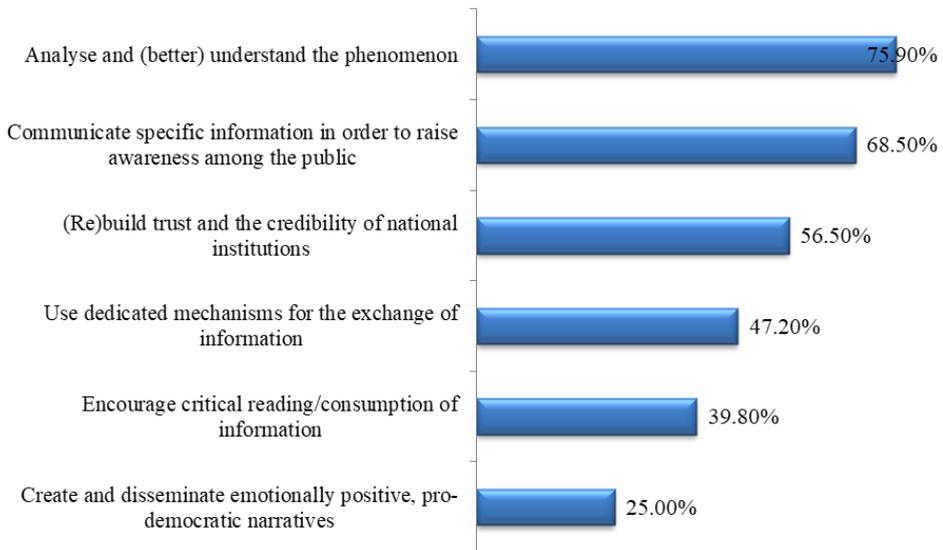


Figure 4: Efficient counteractions or preventive actions
(Source: the author)

When dealing with fake news, the participants to the study evaluate as efficient counteractions or preventive actions: sending the reader to official sources, discrediting the author of the hoax, collaborating with partners for disseminating the answer to fake news, relying on valid sources, answering fast and in a credible manner, but also “exaggerating on victories” and “minimizing defeats”. Also, the use of common sense, the reach of reliable sources, or the use of more than one source can contribute to the discarding/ avoiding of fake news.

“Veracity goes first, and speed second.” (Institutional spokesperson)

“We have prepared a series of infographics that we usually publish when we have an emergency. And we inform people only through official sources.” (Institutional spokesperson)

“What we usually do when we find a hoax is to discredit the author of the hoax, make it clear and even ask the rest of the Twitter community to help us corner that user who has put a hoax on the table and which is not true news.” (Institutional spokesperson)

“Well, I would say that we use our common sense when we obtain a piece of information that could be of interest. We have to evaluate both the source and also the information.” (Cybersecurity expert)

In order to verify the sources, the participants to the study mentioned as efficient techniques the use of automated fake news detectors, the activation of plug-ins for blocking fake news and the use of crowd intelligence and expert intelligence.

During **the preparation phase**, before reporting to the public when addressing a security threat or a sensitive issue, the majority of respondents declared that they totally agree and agree that there are necessary actions to be taken, like double fact checking, verifying the assumptions, reaching out to other sources, identifying the gaps, collecting evidence and information disproving the relevant fake news and presenting the information aligned to the social reality. There was, though, a minority of respondents who disagreed with these type of actions, the most indicated being verifying the assumptions (15) and collecting information disproving fake news (19).

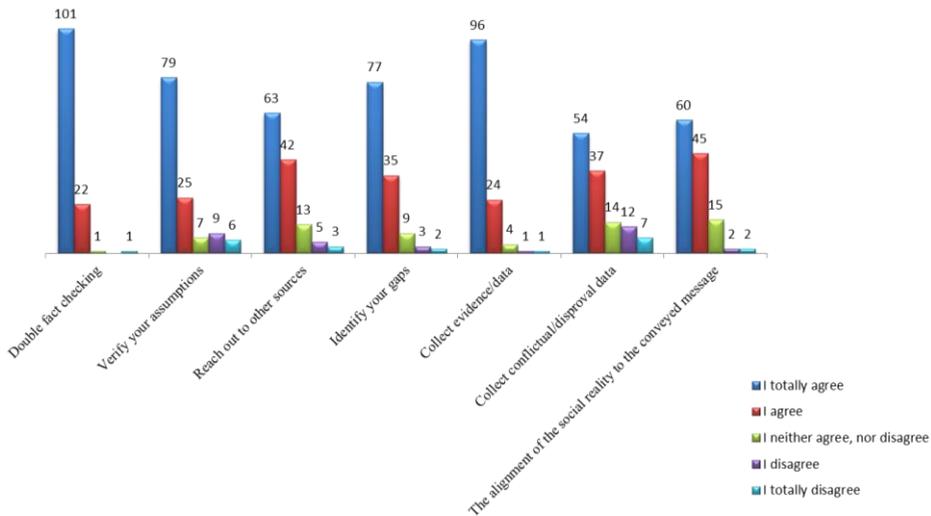


Figure 5: Actions to be taken when addressing a security threat or a sensitive issue (Source: the author)

It is important that the experts in the field are always ready for fake news and threats, are aware of the presence of hoax in social media and become themselves a reliable source for information. During the preparation phase, it is important to include characteristics similar to the ones of the message that has issued a misinformation, so the public can detect easier the false elements. The participants to the study identified as efficient techniques in verifying sources also the use of specialized forums and developing lists of terms used on forums.

“Firstly, giving confidence to the public and to some of our stakeholders. I'm trying to create a narrative trying to explain what happened”. (Academia, Intelligence and security)

“For example, we use some tools to monitor specific sources and we look for a specific list of words in these sources. We have to continuously modify this list of terms.” (Cybersecurity expert)

I use my common sense. [...] My main aim is not to trust immediately the images that I cannot find the origin for. (Journalist)

Also, when reporting on security threats or sensitive issues, the characteristic considered important by the majority of respondents to the questionnaire, in order **to be ethical** (N=124), is truth telling (87, 9%), followed by the preservation of human rights (71, 8%). 18 of the respondents declared that they have at least once found themselves in the situation of having contradictory thoughts on ethical aspects when reporting on security threats or sensitive issues. In such cases, they confronted with contradictory opinions regarding confidentiality of personal data, the principle of competition, or the way it would affect the targeted audience.

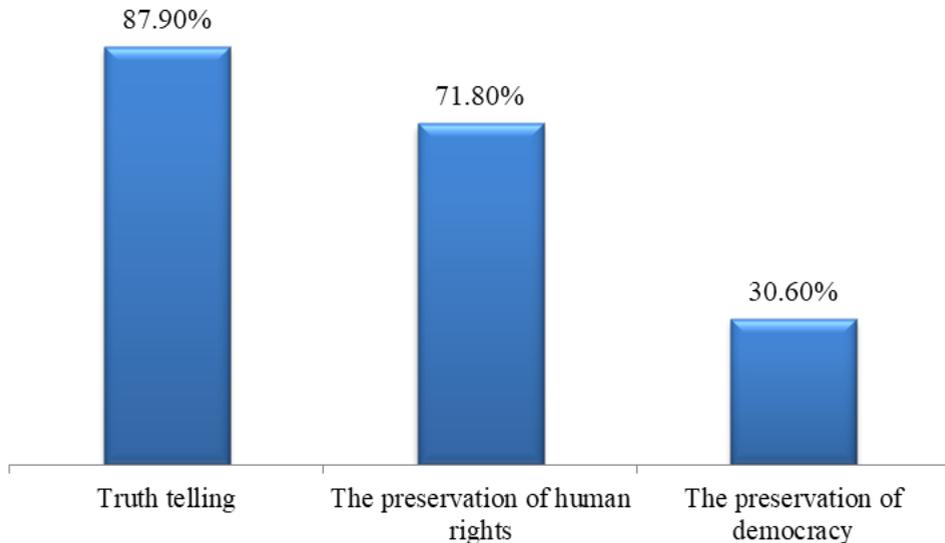


Figure 6: The characteristic considered important to be ethical when reporting on security threats or sensitive issues (Source: the author)

Ethical messages are considered to be able to maintain the balance between the information that is provided without endangering counter-terrorism operations and not causing the increase of hatred. It is also important to rectify possible mistakes and to “give a voice to the victim”. The information must represent the reality, and to be “transmitted with the least possible subjective burden”.

“You need to keep the balance between keeping people informed and not to disrupt counter-terrorist operations, or to create chaos, or to spread hate on other communities.” (Academia)

“Good information (has to be transmitted), not just what you have seen. If you have one photo of something that has happened five minutes ago and some people invent a story about this photo, I would recommend to have a second photo also.” (Cybersecurity expert)

When I work for the news agency, for me, ethics is simple. [...] I have to try to avoid any mistake at all times and especially if I have any mistake in my report I have to rectify as soon as possible. I always have to be honest with my audience, and I have to avoid misleading. [...] My main objective is trying to present the whole picture and trying to give voice to the victims.” (Journalist)

When addressing their own **level of training**, the majority of respondents to the questionnaire evaluated that they can identify actions with negative impact towards the public, or influential/persuasive/manipulative actions. Few of them (less than 20 for each type of action) disagreed or totally disagreed that they can identify these actions – fake news, disinformation, propaganda, polarizing events, hate speech, discrimination, terrorist threats, disaster crisis, radicalization messages, and extremist messages. The type of actions mentioned to be recognized by the most respondents are fake news and disinformation, while hate speech has been indicated by 33 respondents as an action that they can identify. The data indicate a necessity for training in identifying actions such as hate speech, discrimination, terrorist threats, disaster crisis, radicalization messages and extremist messages, as under 50 respondents (out of 127) totally agreed and agreed that they can recognize it.

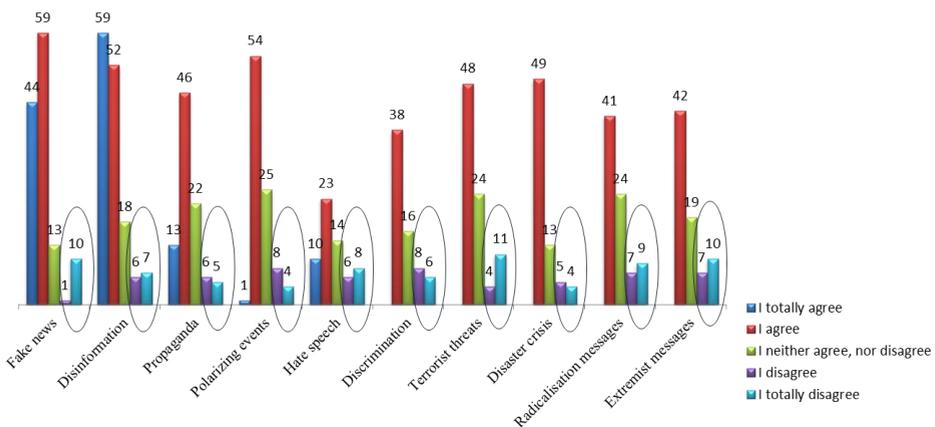


Figure 7: Actions with negative impact towards the public
(Source: the author)

In terms of **further knowledge, skills and competences** that the participants considered necessary for their professional training, in more than 50% of cases (a total of 125 respondents and 542 answers) there were mentioned topics like strategic communication, responsible reaction in relation to the public, and literacy on fake news and related aspects. In less than 50% of cases other aspects were also mentioned: critical thinking strategies, literacy on security issues, developing resilience to fake news and related aspects. In less than 40% of the cases ways of managing public reporting in a responsible way, communicating in case of disaster crisis or ethical reporting, were indicated as topics to be addressed in future trainings.

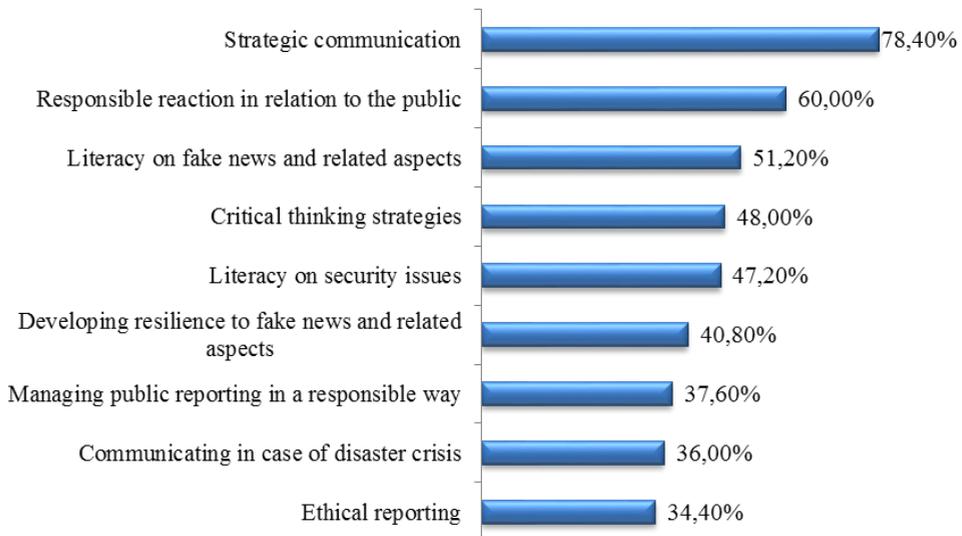


Figure 8: Topics to be addressed in future trainings (Source: the author)

The participants highlighted the importance of literacy into negative actions towards the public, but also the need of practical abilities to analyze, recognize and use tools in relation to it. Also, they highlighted that “journalists must have a clear understanding of the use of terror and racism in the news, in order to differentiate between reporting and manipulating”. An incursion into the legislation, the use

of examples and the development of collaborative abilities are to be taken into consideration for future training.

"I think that propaganda, hate speech, fake news..., especially in the case of fake news, they use a very direct language, they appeal to people's emotions, their messages are very simple and they address not the mind, but the heart, they are very emotional. People tend to believe those fake news easier. It would be great to find a way to report on the truth with the same kind of tools or resources that fake news use." (Journalist)

"I believe that a European and an international policy regarding the education on media and digital literacy, from the levels of young pupils to university students, is urgent and necessary. Digital media literacy includes aspects of reception, production, dissemination of information, as well as critical thinking, communication ethics, protection against misinformation and fake news, among others." (Academia)

"Learning and training is totally necessary, as we have seen in practice that ignorance can lead to the use of stereotype words, intensifying the problem of racist violence. Especially journalists and politicians should be very careful and use a specific terminology instead of an abusive speech. They should exercise more their critical thinking." (NGO)

"Training, especially for junior professionals in strategic communications are vital. Good practices should be taught by professionals that have dealt with crises successfully in the past. I have been in a training where X explained how they dealt with the terrorist attack, which I found very enlightening. In addition, many public figures, like politicians, are managing their own communication, often making many mistakes in terms of sensitivity and political correctness and misinformation." (Community manager)

"I think that the ones involved in communication from public institutions should learn how to communicate. It is important that in a moment of crisis they find a transparent means of communication and designate a person to speak frequently and constantly." (Journalist)

Conclusions

Security threats or sensitive issues are, for the majority of the participants to the study, activities that endanger persons or communities, or the state, that lead to media crisis, to the deterioration of the institution's image, or the propagation of faulty messages regarding the interventions and missions. The clarity, the concise nature and the truthfulness of the message are considered to ensure the success of the reporting activity, while the possibility that the public does not understand the targeted message, provoking panic, or presenting the issue as a generalized matter, are seen as risks when reporting on security or sensitive issues.

A positive response to a reporting activity on security threats or sensitive issues is considered to be the result of focusing on three aspects at the same time, which refer to the content and form of the message, the ways of addressing the public, and the presentation of the interventions undertaken by the authorities. Mandatory actions like verifying the information, being concise, offering true information, being prompt and compassionate, or ensuring the population of the efficacy of the interventions were highlighted by the participants to the study as aspects that lead to the efficiency of the message and a positive response from the public. The high level of training of the communicators, concerning procedures, legislation, and interventions in their field of work, and also the good relationship with mass media, are mentioned (among others) as elements of a successful message. The involvement of the communicators and media in (re)building trust of the people in public institutions or in raising awareness regarding harmful actions towards the public, are necessary steps in reducing the spread of actions with a negative impact over the public.

Further training of experts that work in the field of communication in case of security threats may include theoretical knowledge and practical abilities in identifying actions such as hate speech, discrimination, terrorist threats, disaster crisis, radicalization messages and extremist messages. Also, it resulted the necessity for further knowledge, skills and competences on topics such as strategic communication, responsible reaction in relation to the public, fake

news, critical thinking strategies, security issues, and developing resilience to fake news and related aspects.

References:

1. Babbie, E. R. (2013). *The practice of social research*. Belmont, California: Wadsworth Cengage Learning (12th Ed.)
2. Patton, M. Q. (2002). *Qualitative research and evaluation methods*. Thousand Oaks, California: Sage Publications Inc. (3rd Ed.)

GAMES, EXERCISES AND SIMULATIONS

EDUCAȚIE ÎN INTELLIGENCE: METODA WARGAMING (INTELLIGENCE EDUCATION: THE WARGAMING METHOD)

Bogdan TEODOR*

Mihaela TEODOR*

Introducere

Educația în orice domeniu poate deveni interesantă, eficientă și distractivă prin folosirea avantajelor tehnologiei și ale jocurilor în procesul educativ. Utilizarea jocurilor în procesul educațional a devenit o practică generalizată încă din secolul XX, deși simularea și jocurile strategice au fost folosite încă din epoca modernă ca parte a educației în domeniul militar.

Beneficiile utilizării jocurilor și ale tehnologiei sunt multiple, fapt remarcat de practicienii în domeniu: disciplină, prin impunerea unui setul de reguli; interacțiunea între participanți care are loc aproape continuu, printr-un sistem de feedback; obiectivul jocului sau condițiile necesare victoriei sunt foarte clar definite și cunoscute de către toți jucătorii. (Vezi detalii pe *Cum poți folosi avantajele GaMifIcAtiOn în Educație?*, 16 iunie 2020)

Și în studii de securitate și intelligence se pot utiliza diverse metode bazate pe tehnologie și jocuri, una dintre acestea fiind metoda wargaming, pe care ne propunem să o prezentăm pe scurt în acest material, împreună cu beneficiile pentru educația în intelligence.

Primul pas este reprezentat de înțelegerea corectă a conceptului de wargaming, termen folosit, în special, în domeniul militar. Din cauza asocierii sale, în mod greșit, cu ideea de „joc” a fost adesea insuficient

*Lector univ. dr. în cadrul Academiei Naționale de Informații „Mihai Viteazul”, email: teodor.bogdan@animv.eu

* Cercetător în cadrul Academiei Naționale de Informații „Mihai Viteazul”, email: teodor.mihaela@animv.eu

definit și chiar marginalizat, în ciuda importanțelor beneficii pe care, aplicarea acestei metode le poate aduce în educația în intelligence, și nu numai. Adesea, conceptul de wargaming este înlocuit cu cel de „simulare” sau este folosit în asociere cu alți termeni, precum „teatru de operațiuni” sau „cursul acțiunii”, pentru a câștiga gravitate și credibilitate. Deși împărtășește aspecte cu simularea, în general, wargamingul subliniază în mod explicit valoarea adăugată pedagogică a distracției și a competiției specifică jocurilor.

În prezent, există tendința de a utiliza în locul wargaming-ului conceptul de „serious gaming” (jocuri serioase)¹, sugerând o metodă proiectată în alt scop decât cel al „jocului” și pentru a sublinia componenta gravă a acestui tip de exerciții.

Scurtă istorie

Conceptul de wargame a apărut în secolul al XIX-lea. În urma anglicizării termenului german „kriegsspiel”, care înseamnă „războiul ca un joc”, cuvântul wargame a fost folosit pentru prima dată în Prusia anului 1820, atunci când, doi ofițeri prusaci, von Rechwitz și fiul său, au dezvoltat un set de instrucțiuni pentru reprezentarea manevrelor tactice sub pretextul unui joc. (*Wargaming handbook*, 2017) În anul 1824, conceptul a fost prezentat generalului von Muffling, șeful Statului Major prusac, care, la rândul său, l-a introdus în terminologia militară, metoda fiind folosită pentru instruirea ofițerilor. În următoarele două secole, forțele armate ale majorității națiunilor europene au folosit diferite forme de jocuri pentru instruire și planificare, jocurile de război fiind acceptate ca practică generală, în domeniul militar, până la jumătatea secolului XX și de aici preluate în domenii, precum studiile de securitate și intelligence. (*Wargaming handbook*, 2017)

¹ Jocurile serioase, chiar dacă sunt distractive și antrenante, sunt proiectate în alt scop: pentru instruirea sau educarea jucătorului, cu privire la un anumit subiect sau pentru sprijinirea acestuia, în investigarea unei zone sau promovarea unei cauze. Jocurile serioase au fost dezvoltate într-o serie de domenii, inclusiv apărare, educație, explorare științifică, îngrijire medicală, management de urgență, planificare urbană, inginerie, politică și religie. Vezi detalii pe <https://cs.gmu.edu/~gaia/SeriousGames/index.html>

Încă de la început, s-a considerat că războiul reprezintă o chestiune mult prea gravă, pentru a fi tratată ca un simplu „joc” și s-a ajuns astfel, la varianta wargaming înțeleasă ca „exercițiu de război utilizând mecanismele jocului”, care implică existența unor reguli, obiective, scenarii, procese, jucători, arbitri, analiza, incertitudinea, șansa/norocul. Termenul de *jucători* este adesea înlocuit cu „public specializat” sau „echipă de investigații”. (*Wargaming handbook*, 2017)

Componente

Atunci când ne referim la wargame, trebuie să avem în vedere: elementele constitutive; diferitele tipuri ale acestei metode; scopul urmărit și modul de aplicare. Cunoașterea acestor componente stă la baza capacității de a realiza produse analitice de succes. Condițiile enumerate anterior conduc spre identificarea celor **șapte elemente, identificate drept componente principale ale wargaming-ului, reprezentate în figura alăturată** (*Wargaming handbook*, 2017, p. 8):

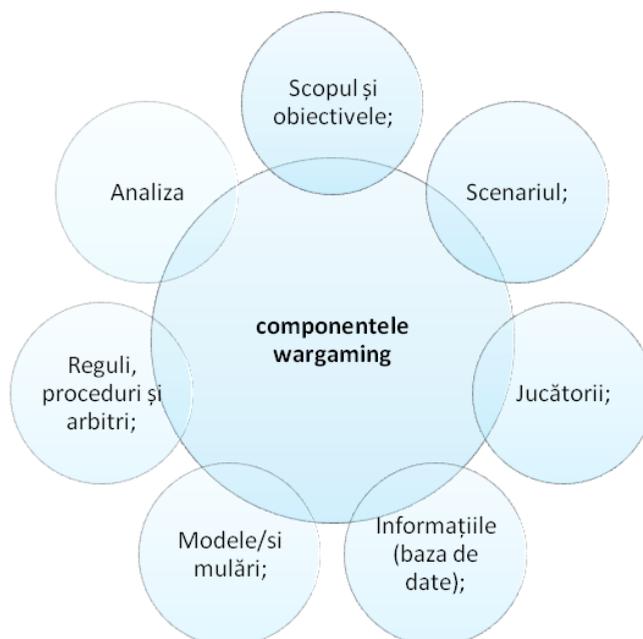


Figura 1: Componentele wargaming-ului
(Sursa: *Wargaming handbook*, 2017, p. 8)

Scopul și obiectivele; scenariul; jucătorii; informațiile (baza de date); modelele/simulările; regulile, procedurile și arbitrii; analiza, constituie componentele wargaming-ului dar nu îl definesc. Cel mai adesea definițiile wargaming-ului, cuprinse în doctrine, sunt imprecise. Termenul a fost introdus în glosarul NATO, începând cu anul 2000, fiind definit astfel: „Simularea, prin orice mijloace, a unei operațiuni militare care implică două sau mai multe forțe oponente, utilizând reguli, date/informații și proceduri concepute pentru a descrie o situație reală sau presupus reală.” (NATO Glossary of terms and definitions AAP-6, 2008, p. 235)

Această definiție include unele dintre elementele componente ale wargaming-ului, dar pentru că poate fi aplicată oricărui tip de activitate sau operațiune militară este prea largă pentru a fi utilă în domeniul educației în intelligence. O definiție mai completă este cea oferită de Peter Perla, specialist în cercetarea aplicațiilor de tip wargame, în lucrarea sa *The Art of Wargaming*, în care consideră wargaming-ul ca fiind: „un model sau o simulare de război, care utilizează reguli, date/informații și proceduri, fără a implica forțe militare reale, și în care fluxul de evenimente este afectat, și la rândul său influențează, deciziile adoptate în cursul desfășurării aplicației de către jucători, reprezentând părțile oponente.” (Perla, 1990, p.274)

Asemănător este definit acest concept și de către specialiștii din cadrul Centrului pentru Dezvoltare, Concepte și Doctrină, think-tank al Ministerului Apărării din Marea Britanie, în care „rezultatul și succesiunea evenimentelor afectează și sunt afectate de deciziile luate de jucători”. (Wargaming Handbook 2017, p. 5) Specialiștii britanici definesc wargamingul astfel: „Metoda wargame este o simulare a aspectelor selectate ale unei situații de conflict, în conformitate cu regulile, datele și procedurile prestabilite pentru a oferi experiență și informații decizionale care se aplică unor situații din lumea reală”. (Wargaming Handbook 2017, p. 10)

Pornind de la elementele principale identificate în cadrul definițiilor prezentate, putem afirma că, în prezent wargaming-ul este definit ca o reprezentare a activităților militare, contradictorii prin natura lor, ce utilizează reguli, date și proceduri specifice, fără a implica forțe militare reale, și în cadrul cărora fluxul de evenimente este afectat,

și la rândul său afectează, deciziile adoptate de către jucători, care acționează în numele diverșilor actori, facțiuni, factori, relevanți pentru acest tip de activitate. (*Wargaming handbook*, 2017)

Wargaming și educație în intelligence

Pentru a răspunde la întrebarea „câte tipuri de wargame sunt?” am preluat următoarea diagramă, care ilustrează o taxonomie simplă a conceptului de wargame, introducând în același timp idea că toate tipurile de wargame sunt în strânsă legătură cu zona suportului decizional și cea a factorilor de decizie:

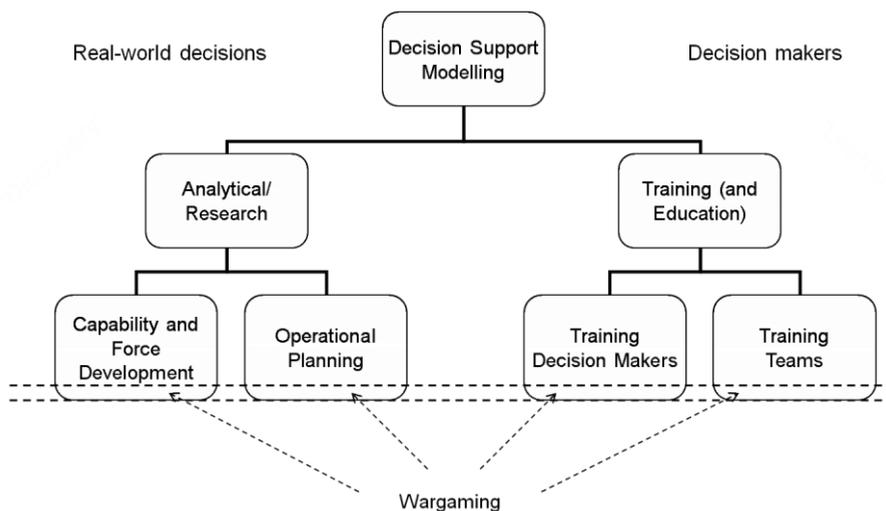


Figura 2: Taxonomie a conceptului de wargame
(Sursa: <http://lbsconsultancy.co.uk/our-approach/what-is-it/>)

În funcție de domeniul în care sunt utilizate, aplicațiile de tip wargaming pot fi diferite, dar indiferent de contextual în care sunt utilizate, aceste aplicații ar trebui să permită factorilor de decizie să înțeleagă mai bine procesul de luare a deciziilor. Scopul aplicației de tip wargaming poate fi și doar o înțelegere aprofundată a procesului de adoptare a deciziei. Scopurile urmărite, atunci când aplicația de tip wargaming se adresează zonei de pregătire și educație, pot fi diferite,

dar se subsumează preocupărilor privind îmbunătățirea capacității de adoptare a deciziilor, atât pentru echipa de comandă, cât și la nivelul personalului.

Obiectivul general pe care îl urmărește o aplicație de tip wargaming este acela de a introduce toți participanții într-un mediu controlat, care să îndeplinească cerințele minime de realism, pentru a îmbunătăți capacitatea acestora de luare a deciziilor sau de a identifica cea mai bună soluție pentru o problemă reală.

Obiectivele specifice ale fiecărei aplicații de tip wargaming depind de specificitatea fiecărui eveniment ce face obiectul aplicației. Acest obiectiv poate merge de la îmbunătățirea capacității echipei de comandă a unei unități militare, de a adopta decizii în lipsa unor informații și până la suportul acordat factorului de decizie, în adoptarea hotărârii de a instala elemente ale unui scut antirachetă pe teritoriul național.

În domenii precum analiza de intelligence obiectivele ce trebuie avute în vedere sunt, în linii generale, următoarele:

- Identificarea riscurilor și disfuncționalităților ce pot interveni în alcătuirea unui plan de analiză;
- Validarea ipotezelor în scopul dobândirii de noi date de cunoaștere despre factorii ce pot influența adoptarea unei anumite decizii;
- Sporirea încrederii factorului de decizie, prin oferirea unui produs valid.

Etape ale aplicației de tip wargame

Principalul obiectiv al unei aplicații de tip wargaming în educația în intelligence este de a dezvolta capacitatea de analiză a studenților, poziționându-i în situația de a juca un rol pentru a manageria o situație ipotetică în care este amenințată securitatea națională. Pentru zona de pregătire și educație în intelligence realizarea unei aplicații de tip wargaming trebuie să parcurgă următoarele șapte etape:

- ✓ Formularea scopului și a obiectivelor de formare urmărite;

- ✓ Selectarea persoanelor ce urmează să participe la aplicație, stabilirea rolului pe care urmează să-l îndeplinească și a deciziilor ce urmează să le adopte;
- ✓ Stabilirea activităților în care jucătorii vor fi implicați și efectele ce se doresc a fi obținute;
- ✓ Realizarea scenariului și precizarea tipului și surselor de informații pe baza cărora jucătorii vor adopta decizii, pentru atingerea obiectivelor de formare propuse;
- ✓ Stabilirea resurselor și proceselor necesare pentru a realiza pașii 3 și 4;
- ✓ Identificarea instrumentelor și tehnologiei necesare pentru a permite realizarea proceselor propuse;
- ✓ Realizarea unui sistem de audit care să permită documentarea deciziilor adoptate și motivarea acestora.

Munca analiștilor seamănă în multe privințe cu cea a cercetătorilor științifici. Ei formulează ipoteze, operaționalizează concepte, sunt preocupați de presupuneri, analizează date, le interpretează și le integrează, distinge între problemele majore și cele minore, trasează concluzii și încearcă să le prezinte concluziile cât se poate de clar. În cazul aplicațiilor realizate pentru domeniul analiză și cercetare, pașii ce trebuiesc urmați sunt următorii:

- Formularea scopului, astfel încât să includă obiectivul general al cercetării, și obiectivele specifice urmărite;
- Identificarea obiectului analizei, precum și a posibilelor erori ce pot surveni;
- Stabilirea modului în care se va face evaluarea obiectului analizei, scenariile necesare și variabilele ce trebuiesc luate în calcul pentru realizarea analizei;
- Stabilirea modului în care se va face colectarea datelor și evaluarea acestora;
- Identificarea persoanelor care vor realiza validarea rezultatelor analizei;
- Stabilirea ipotezelor de lucru;
- Identificarea proceselor necesare pentru realizarea obiectivelor;
- Identificarea instrumentelor și tehnologiei necesare pentru a permite realizarea proceselor propuse;

- Realizarea unui sistem de audit care să permită documentarea deciziilor adoptate și motivarea acestora.

Acest tip de aplicație poate fi derulat ori de câte ori contextul o impune, intervalul de timp necesar fiind flexibil. Pot participa studenți, dar și masteranzi cu pregătire în domeniile intelligence, securitate națională și relații internaționale. Multe dintre recomandările metodologice pentru analiza de intelligence sunt împrumutate din arsenalul metodologic de cercetare științifică din diferite domenii precum istoria, relațiile internaționale, studiile de comunicare și jurnalism, sociologia, științele politice și studiile de securitate etc. (De Graff, 2019)

Beneficii și limitari ale aplicației de tip wargame

Între beneficiile aplicațiilor de tip wargaming este faptul că oferă **medii structurate și în condiții sigure în caz de eșec, pentru a explora**, de obicei cu un cost relativ redus, ceea ce funcționează și ceea ce nu funcționează în diverse situații. Mai mult, acestea oferă un **cadru dinamic determinat de deciziile jucătorilor, care permite învățarea activă**: jucătorii se confruntă cu întrebări și provocări continue și deseori neașteptate, în timp ce explorează, experimentează și concurează în cadrul modelului artificial pe care îl oferă jocul. (*Wargaming handbook*, 2017) Alte avantaje ar fi: oportunitate de a explora opțiunile și de a-și asuma riscuri, fără a risca vieți sau a perturba continuitatea activității de intelligence; un mod rentabil de a practica comanda și de a exercita abilitățile de management; expunerea la fricțiuni și incertitudine; un mecanism de explorare a inovării în arta războiului; și o metodă pentru descoperirea unor factori și întrebări noi. (*Wargaming handbook*, 2017)

Între limitări, specialiștii britanici au recunoscut faptul că, aplicațiile de tip wargaming nu sunt reproductibile. Niciun joc nu va fi niciodată același, chiar și atunci când situația de pornire este replicată, evoluția lor fiind determinată de deciziile jucătorilor, alegerile acestora fiind diferite chiar și atunci când li se prezintă aceeași situație. (*Wargaming handbook*, 2017)

Desigur, tocmai imprevizibilitatea, cuplată cu creativitatea participanților, este cea care permite ca aplicațiile de tip wargame să

genereze idei noi. Dar tocmai faptul că output-urile aplicațiilor de tip wargame sunt doar calitative nu și cantitative reprezintă o altă limitare. O altă limitare este și faptul că nu sunt predictive. Wargames ilustrează rezultatele posibile sau plauzibile, dar nu va putea prezice definitiv că este probabil, astfel încât există riscul de a fi identificate lecții false. Mai mult, calitatea aplicației depinde de calitatea jucătorilor. Astfel, expertiza și o mai mare diversitate aplicate în rândul participanților poate genera o perspectivă solidă asupra temei aplicației de tip wargame.

Referințe:

1. *** NATO Glossary of terms and definitions AAP-6, 2008.
2. *** Wargaming Handbook. (2017) *Development, Concepts and Doctrine Centre UK*, disponibil la https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/641040/doctrine_uk_wargaming_handbook.pdf
3. Birnstiel, Marc; Kämmerer, Michael; Kern, Stefan; May, Thomas; Noeske, Andreas; Matthew Caffrey, *History of Wargames: Toward a History Based Doctrine for Wargaming*, 2000, disponibil la <http://www.strategypage.com/articles/default.asp?target=WARGHIS2.htm>
4. *Cum poți folosi avantajele Gamification în Educație?*, 16 iunie 2020, accesibil la <https://targeton.ro/blog/cum-poti-folosi-avantajele-gamification-in-educatie>
5. De Graff, Bob, (2019), *Intelligence and Intelligence studies. Time for a divorce?*, in Romanian Intelligence Studies Review, no. 21/2019, pp. 7-30.
6. Development, Concepts and Doctrine Centre (DCDC), *Red Teaming Guide: A scenario-based warfare model*, 2nd Edition, 2013.
7. Peter Perla, *The Art of Wargaming*, Naval Institute Press, 1990.
8. Peter P. Perla, ED McGrady, *Why Wargaming Works*, *Naval War College Review*, Summer 2011, Vol. 64, No. 3.
9. Reershemius, Ingo; Seglitz, Christoph; Walther, Marc-André, *Wargaming - Guide To Preparation And Execution*, Hamburg, 2006.
10. Sabin, Philip, 2015, *Wargaming in Higher Education*, Arts and Humanities in Higher Education.
11. *What is Wargaming?*, disponibil la <http://lbsconsultancy.co.uk/our-approach/what-is-it/>

REVIEWS AND NOTES

**Simon Sinek *Leaders Eat Last:
Why Some Teams Pull Together and Others Don't***

Publica Publishing House, Bucharest 2014,
translated by Gabriel Crețu

Review by Valentin NICULA*

The present review tries to highlight the work and results of Simon Sinek in the paper entitled *Leaders Eat Last: Why Some Teams Pull Together and Others Don't*, published by Publica Publishing House (Bucharest 2014, ISBN 978-606-8360-94-2, the Romanian version translated by Gabriel Cretu under the title *Liderii mânăncă ultimii: de ce unele echipe lucrează bine împreună, iar altele nu*) in an atypical approach, from the perspective of a reader trying to put into practice the principles derived from the book, rather than following the classic structure of a review. Therefore, the presentation is intended to be more of a *teaser* and an invitation to read, than a review *per se*.

"If your actions inspire others to dream more, to learn more, to do more, and to become something more than they are, then you are called a leader", is the quote considered as the key message of the book by George J. Flynn (Lt.-gl. in the US Marine Corps), the person who prefaces the book. The US general's explanation is that "when leaders **inspire** those they lead, people think of a better future, invest time and effort to learn more, do more for their organizations, and become **leaders** themselves along the way."

If the key process described by the US Army general is "**inspiration**", in my opinion the key process described by the book is **to build trust** between people, as members of a team or organization, in a broad sense. Without trusting the person next to you, your co-

* Researcher PhD within "Mihai Viteazul" National Intelligence Academy, nicula.valentin@animv.eu

worker and especially, without trusting your leader/boss (who is supposed to be able to show you the path you must follow in your work), a team's actions cannot see long-term success. **Trust** provides security and success through **cooperation** in achieving goals.

Although we are living in a not so happy period, characterized by pessimistic forecasts that surround our existence at every click or new tab opened in the news apps, I consider that an approach from an **optimistic** perspective of inter-human relations, as they are presented by Simon Sinek, can represent the **competitive advantage** through which people and organizations alike can overcome both present and future moments of crisis.

During the present review I do not intend to offer definitions and explanations about the relationship between the "altruistic hormones" (serotonin and oxytocin) and the "selfish" ones (endorphins and dopamine) or about the role of "cortisol" in human existence since ancient times. One can find all these explanations in the chapters of the book *Leaders Eat Last*.

Whether it is read on a deck chair during summer vacation, in the shade of a tree in the park on weekends, or with a pen in hand and a notebook, as a compulsory reading contained in a curricula of a management and leadership course, I can assure the future readers that the book is captivating, combining in a totally non-precious way scientific data and explanations with relevant stories and anecdotes.

Although at first glance it may seem just another paper of those hundreds (even thousands) works in the area of management, which promise immediate successful solutions by following a pre-defined recipe, Sinek's book advances a **paradigm shift**, "a beginning for each of us", as the translator of the Romanian edition, Gabriel Crețu, concludes his intervention.

It is a useful new beginning for leadership in both private and public areas, at all levels and areas of specialization, including the military and security ones. Not coincidentally, the book is dedicated to men and women in the US Air Force and the author provides as examples for the principles stated out short stories and accounts of events from the battlefield, not just from the offices of successful big companies.

ACADEMIC FOCUS



Strategic partnership project within
ERASMUS+ Program
AGREEMENT No. –
2018-1-RO01-KA202-049449

**MIND THE GAP IN MEDIA
COVERAGE AND STRATEGIC
COMMUNICATION IN CASE
OF SECURITY THREATS –
THE DEVELOPMENT
OF CRITICAL THINKING
AND RESPONSIBLE REACTION**
(October 1st, 2018 –
September 30th, 2021)

CRESCent project addresses the challenge of social polarization created by the propagation of disinformation and fake news. It is a proven fact that fake news have created in Europe, and in the three countries participating in the project, an acute miscommunication and lack of trust between the two targeted professional categories. As the media has been pressed into reaching large audiences, institutional spokespersons were forced into communicating what is necessary and not divulging aspects which could jeopardise security investigations and public safety. A gap of trust and efficient communication was, thus, created and later on widened by the phenomenon of fake news. While it is indeed the media professionals that shape the way information is delivered to the public, they themselves might get trapped in particular “narratives” and share common mental frames. Recognizing that the media professionals are themselves the locus of potential influence by external actors is crucial to developing strategies to combat misinformation and hostile influence. CRESCent aims to address this divide through innovative solutions and multiplication of best practices of both spokespersons and journalists.

CRESCent project creates a training platform and a set of communication and cross-sectorial strategic communication instruments, which aim to capacitate institutional spokespersons and journalists from security and LEA fields, in order to use media reporting

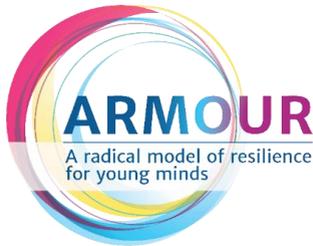
to the public in a conscious and ethical manner. CRESCent's main target group consists of spokespersons in the field of national security and LEAs. The secondary group is represented by (young) journalists who are active in the field of security.

Participating organizations are: "Mihai Viteazul" National Intelligence Academy (MVNIA) – Romania; University "Rey Juan Carlos" (URJC) – Spain; Kentro Meleton Asfaleias (KEMEA), Centre for Security Studies – Greece; Ministry of Internal Affairs, Directorate for Information and Public Relations (MAI-DIRP) – Romania.

Objective of the project are:

- to develop a toolkit of techniques, methods and instruments for institutional spokespersons and journalists who communicate on issues related to security and law enforcement, as support in their professional activity;
- to enhance key-competences and skills of the spokespersons and journalists so that they become resilient to fake news, build an ethics of reporting, perform double fact checking, provide and obey ethical grounds in handling sources, report security threats and handle truth for the preservation of democracy and the rule of law.

The CRESCent project is part of the ERASMUS+ program and it is funded by the European Commission. See more about the project on the official website: <https://crescentproject.eu>



**A RADICAL MODEL OF RESILIENCE
FOR YOUNG MINDS – ARMOUR**
Grant Agreement No. 823683
(January 1st, 2019 – December 31st, 2021)

The Euro-Arab Foundation leads ARMOUR (*A Radical Model of Resilience for Young Minds*) consortium and the project aiming to address the social polarization caused by the adoption and spread of extremists ideologies by creating an interdisciplinary learning model that helps individuals and communities develop resilience to the specific ideologies and behaviours of violent extremism. The ARMOUR's consortium, led by the Euro-Arab Foundation, is also made up of the Centre for Security Studies – KEMEA (Greece), the “Mihai Viteazul” National Intelligence Academy (Romania), SYNYO GmbH (Austria), the Italian Ministry of Justice, Agenfor (Italy), LIBRe Foundation (Bulgaria), the University of Malta (Malta) and the University of Groningen (Netherlands).

ARMOUR Project aims to address societal polarization via strengthening resilience of individuals, communities and vulnerable groups (such as children, youth etc.) to polarisation, and to promote interaction and cooperation between different local actors from public sectors, i.e. law enforcement, social services etc., that specialise in working with vulnerable groups in preventing extremism through development of cooperation models. The project will design and create a Toolkit for first-line practitioners to employ in reducing polarization among children and youth.

The Toolkit, capitalizing on previous work carried out by project partners, takes the form of experimental laboratories (experimental labs) which together work towards: strengthening individual capacity to resist push and pull factors of radicalization; creating community empowerment and resilience to social polarization and violent

extremism and assisting states deploy proportional responses against provocations and latent conflicts. The model will then be promoted through a social media campaign.

The expected impact of the project covers the following aspects:

- Increasing awareness and capacity of first-line practitioners: ARMOUR achieves this through the experimental labs and the related training programme. The first tool will help practitioners better understand and identify instances of radicalization and polarization among children and youth while the second one will help them improve their ability to use the project toolkit;
- Promoting interaction and cooperation among different stakeholders: ARMOUR achieves this by organizing the experimental labs in which practitioners and members of vulnerable communities have trusted interactions;
- Promoting the views of moderate voices by engaging with the silent majority and integrating them into the experimental lab;
- Developing and promoting concrete tools targeting vulnerable groups: the experimental lab combined with the best practices identified in the project and the online campaign are concrete tools which key actors can use when working with vulnerable youth.

The project is financed by the Internal Security Fund, a funding package of the Directorate-General for Home Affairs (European Commission) to promote the implementation of the Internal Security Strategy, law enforcement cooperation and the management of the Union's external borders. See more about the project on the official website: <https://armourproject.eu/a/privacy-policy>

Iceland
Liechtenstein
Norway grants

THESEUS

Connect the Disconnections -
from Disparate Data to Insightful Analysis



**Education, Scholarships, Apprenticeships
and Youth Entrepreneurship
Programme in Romania, funded by the EEA Grants -
Financial Mechanism 2014-2021**

Agreement no.: 18-COP-0017

(October 1st, 2019 – September 30th, 2021)

THESEUS Project aims at Connecting the Disconnections between Disparate Data, in order to provide knowledge for building Insightful Analysis. The broad availability of data has led to increasing interest in methods for extracting useful information and knowledge from data, determining the emergence of new fields of science (e.g. data science). At the same time, big data algorithms have been signaled as a potential leverage that can lead to digital dictatorship if insufficiently understood, poorly handled and unethically regulated. Companies in every industry focused on ways to structure, process and analyze the growing volume and diversity of data so as to streamline decisions and gain a competitive edge. State institutions, regular citizens, social and political science practitioners on the other hand, are not yet properly equipped to properly mitigate the economic, social and political impact of the information technology revolution that awaits us in the decades to come. Therefore, in the process of understanding and mitigating risks and opportunities of Big Data, complex workloads, new skills and competences have to be acquired.

Following these emerging needs, the **objective of the project** is to enhance human capital and knowledge base by tackling directly skills and competences required and providing an understanding of the

processes guiding big data analytics. This objective will be met by **building and delivering a course**, consisting of four modules, capitalizing on big data methodologies: introductory module, data collection module, data processing module and data analysis module.

The course will not be designed as a technologically focused course, but rather a knowledge, awareness and understanding focused course. The course avoids an algorithm-centered approach. It focuses on how options are understood and choices and tradeoffs are designed. Thus, it enhances, through learning by doing, key-competences and skills required in collecting, understanding, correlating and processing big data, helping them streamline problem-solving processes in a data-driven ecosystem.

The project addresses **two professional categories**: *governance and social scientists* and *national security practitioners*, whose complementary work is of paramount importance in insuring the sustainable development of democracy. Both categories carry out great responsibility at social level. Ill-informed decisional processes in national security and policy-making, based on incomplete, inaccurate or incorrectly correlated data generate negative impact, affecting society at large. Although practitioners targeted by the project work with large amounts of data, their background is mostly in social science or security studies, lacking a very specific technical training. Such (future) professionals need to better understand what and how big data can be capitalized so as to ethically and lawfully improve the overall efficiency of their organization.

Participating organisations are: “Mihai Viteazul” National Information Academy (ANIMV) – Romania; University of Malta (UoM) – Malta; Norwegian University of Science and Technology (NTNU) – Norway; National University of Political Studies and Public Administration (SNSPA) – Romania. THESEUS Project is part of the Education, Scholarships, Apprenticeships and Youth Entrepreneurship Programme in Romania, being funded by the EEA Grants – Financial Mechanism 2014-2021.



**Empowering a Pan-European
Network to Counter Hybrid
Threats (EU-HYBNET)
H2020 Grant agreement
no: 883054
(May 2020 – April 2025)**

EU-HYBNET is a 60 month project (2020-2025), financed through the Horizon 2020, which will start in May 2020. The project is being developed and implemented by a consortium of 25 partners, coordinated by LAUREA University of Applied Sciences from Finland. The European Centre of Excellence for Countering Hybrid Threats and the Joint Research Centre are leading partners of the EU-HYBNET project.

EU-HYBNET will bring together practitioners and stakeholders to identify and define their most urgent requirements for countering hybrid threats, by undertaking an in-depth analysis of gaps and needs and prioritizing those that are crucial to address through effective research and innovation initiatives, including arranging training and exercise events to test the most promising innovations (technical and social) which will lead to the creation of a roadmap for success and solid recommendations for uptake, industrialization and standardization across the European Union.

The project aims to build an empowered, sustainable network, which will:

- define common requirements that can fill knowledge gaps, deal with performance needs, and enhance capabilities of innovation endeavors;
- monitor significant developments in research and innovation;

- deliver recommendations for uptake and industrialization of the most promising innovations that address the needs of practitioners, and determine associated priorities for standardization;
- establish conditions for enhanced interaction among its members;
- persistently strive to increase its membership and continually build network capacity through knowledge exchange.

EU-HYBNET will address four core themes to ensure coherence in the project's results: 1) Future Trends of Hybrid Threats, 2) Cyber and Future Technologies, 3) Resilient Civilians, Local Level and National Administration, and 4) Information and Strategic Communication.

Romania represents the consortium through "Mihai Viteazul" National Intelligence Academy (MVNIA). MVNIA will incorporate the project's research findings and information into its MA & PhD research programs. As students come from diverse areas (security practitioners, legal, media, private business), the impact of exploitation of the information will reach a wide audience, and the EU-HYBNET training documents will also be employed to enhance capabilities of experts and practitioners in the fight against hybrid threats.

EU-HYBNET is a Pan-European network of security practitioners, stakeholders, academia, industry players, and SME actors across EU, collaborating with each other to counter hybrid threats.

CALL FOR PAPER ROMANIAN INTELLIGENCE STUDIES REVIEW

“Mihai Viteazul” National Intelligence Academy, via its National Institute for Intelligence Studies, publishes the *Romanian Intelligence Studies Review* (RISR), a high quality peer reviewed and indexed research journal, **edited in English and Romanian twice a year.**

The aim of the journal is to create a framework for debate and to provide a platform accessible to researchers, academicians, professional, practitioners and PhD students to share knowledge in the form of high quality empirical and theoretical original research papers, case studies, conceptual framework, analytical and simulation models, literature reviews and book review within security and intelligence studies and convergent scientific areas.

Topics of interest include but are not limited to:

- Intelligence in the 21st century
- Intelligence Analysis
- Cyber Intelligence
- Open Source Intelligence (OSINT)
- History and memory in Intelligence
- Security paradigms in the 21st century
- International security environment
- Security strategies and policies
- Security Culture and public diplomacy

Review Process: RISR shall not accept or publish manuscripts without prior peer review. Material which has been previously copyrighted, published, or accepted for publication will not be considered for publication in the journal. There shall be a review process of manuscripts by one or more independent referees who are conversant in the pertinent subject area. Articles will be selected based on their relevance to the journal's theme, originality and scientific correctness, as well as observance of the publication's norms. The editor evaluates the recommendation and notifies the author of the manuscript status.

The review process takes maximum three weeks, the acceptance or rejects notification being transmitted via email within 5 weeks from the date of manuscript submission.

Date of Publishing: RISR is inviting papers for No. 25 and 26 and which is scheduled to be published on June and December, 2021.

Submission deadlines: February 1st and July 1st

Author Guidelines: Author(s) should follow the latest edition of APA style in referencing. Please visit www.apastyle.org to learn more about APA style, and <http://www.animv.ro> for author guidelines. For more details please access the official website: **rrsi.ro**

Contact: Authors interested in publishing their paper in RISR are kindly invited to submit their **proposals electronically in .doc/.docx format at our e-mail address rrsi@sri.ro, with the subject title: RRSI article proposal.**

Appearing twice a year, the review aims to place debates in intelligence in an institutional framework and thus facilitating a common understanding and approach of the intelligence field at national level.

The target audience ranges from students to professionals, from the general public to those directly involved in intelligence research and practice.

ISSN - 2393-1450
ISSN-L - 2393-1450

“MIHAI VITEAZUL”
NATIONAL INTELLIGENCE ACADEMY

National Institute for Intelligence Studies

20, Odăi Str.
Bucharest 1 - ROMANIA
Tel: 00 4037 7721 140
Fax: 00 4037 772 1125
e-mail: rrsi@sri.ro

www.animv.ro
www.rrsi.ro