National Institute for Intelligence Studies

RISR No. 19-20/2018

Romanian Intelligence Studies Review



Editura ANIMV

"MIHAI VITEAZUL"
NATIONAL INTELLIGENCE ACADEMY

ROMANIAN INTELLIGENCE STUDIES REVIEW

No. 19-20/2018

The *Romanian Intelligence Studies Review* is an 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
2019

Senior Editors

Adrian IVAN
- Rector of "Mihai Viteazul" National Intelligence Academy, Romania

Michael ANDREGG
- Professor at St. Thomas University, United State of America

Cristian BARNA
- Professor at "Mihai Viteazul" National Intelligence Academy, Romania

Irena CHIRU
- Professor at "Mihai Viteazul" National Intelligence Academy, Romania

Iulian CHIFU
- Professor at The National School of Political and Administrative Studies, Romania

Vasile DÂNCU
- Professor at "Babeş-Bolyai" University from Cluj, Romania

Christopher DONNELLY
- Director of the Institute for Statecraft and Governance, Oxford, Great Britain

Iulian FOTA
- Associate Professor at "Mihai Viteazul" National Intelligence Academy, Romania

Jan GOLDMAN
- Associate Professor of Justice Studies Southern New Hampshire University, Great Britain

Sergiu MEDAR
- Professor at "Lucian Blaga" University from Sibiu, Romania

Ioan Mircea PAŞCU
- Professor at The National School of Political and Administrative Studies, Romania

Mark PHYTHIAN
- Professor at University of Leicester, Great Britain

Elaine PRESSMAN
- Expert at Netherlands Institute for Forensic Psychiatry and Psychology, Netherlands

Board of Editors

Editor in Chief: *dr. Mihaela TEODOR*
Editors: *dr. Valentin NICULA*
dr. Valentin STOIAN

Editorial Secretary: *Lucian COROI*
Cover: *Valentin NICULA*

CONTENT

INTELLIGENCE ANALYSIS 5
Patrick RUS
Exploring unknown unknowns in Intelligence analysis..... 7
Jules J. S. GASPARD
Calling a spade, a spade: a return to 'Counterespionage' from 'Counter-Intelligence 15

OPEN SOURCE INTELLIGENCE (OSINT)..... 31
Mihaela BERBEC
Features of Chinese Intelligence system: experimenting
with metaknowledge 33
Matteo E. BONFANTI
An Intelligence-based approach to countering social media influence operations 47

INTELLIGENCE IN THE 21ST CENTURY 69
Fernando VELASCO, José Ángel GONZÁLEZ
The destabilization of democracies through the spread of disinformation:
the role of Intelligence..... 71
Sabrina MAGRIS, Martina GRASSI, Perla di GIOIA
Intelligence and Counterterrorism: the meaning of words is the right tool
to make an efficient analysis when the threat is hybrid 93

CYBER INTELLIGENCE 107
Alexandra Elena TIMOFTE
Estonia cyber-attacks and the impact on NATO 109
Andrei VLĂDESCU
To be or not to be radical. From online discursive aggressiveness
to offline aggression 125

HISTORY AND MEMORY IN INTELLIGENCE 137
Ioan Codruț LUCINESCU
Soviet espionage actions against Romania in the first interwar decade.
The case study of General Ludovic Mircescu..... 139
Mircea STAN, Florin BUȘTIUC
The importance of the active measures program within the collaboration
and intelligence sharing among Warsaw Treaty Organization member
states' security and Intelligence services against the West and NATO
allies during the cold war 147
Iulia Cristina SACALAS
The industrial espionage, a strategic objective of the Romanian
Communist system between 1965 and 1989 173
Bogdan Alexandru TEODOR, Mihaela TEODOR
Eastern and Central Europe in the cold war period: the Soviet model
of Intelligence structures 191

INTELLIGENCE AND SECURITY IN THE 21ST CENTURY 203
Valentin STOIAN-IORDACHE
A Rawlsian approach to de-securitization 205

Mihai SANDU
The role of the Malacca Strait in the past and current regional and international power relations and security architecture 217
Mircea ORMENISAN
The refugee crisis and how it impacted the European continent..... 229
Michael ANDREGG
Ultimate causes of wars (long-term, strategic causes) and differing roles for Intelligence practitioners, academics, and policy makers 237
Iulian DICULESCU-BLEBEA
A Faustian pact: the regime of truth within national security documents in Romania and Germany 257

SECURITY PARADIGMS IN THE 21ST CENTURY 281
Dragan SIMEUNOVIC
Islamistic extremism and terrorism in the Western Balkans 283
Florian COLDEA
Security and the fight against terrorism as keys to regional stability: Romanian lessons 317
Vasile CREȚU, **Dragoș ARDELEANU**
The revival of the Intermarium geopolitical project - the Three Seas Initiative and Bucharest 9 Format..... 331
Adrian-Vasile POPA
Reconfiguring the balance of power in the wider Black Sea Region: the Romanian proposal for an allied naval cooperation 345
Tetiana IEFYMENKO
Coordination of counteraction to turmoil in the economic space of the Black Sea Region 375

INTELLIGENCE, SECURITY AND INTERDISCIPLINARITY 395
Giangiuseppe PILI
Intelligence and social epistemology: a social epistemological theory of Intelligence 397
Ileana SURDU,
The impact of leisure time policies on economic security 419
Claudia GOGOAȘĂ LASCATEU
The collision between public policy and technology raises the stakes for users..... 433

REVIEWS AND NOTES..... 445
Alina BÂRGĂOANU
#FakeNews. Noua cursă a înarmării, Editura Evrika, 2018, 252p (Recenzie de Mihaela TEODOR)..... 447

ACADEMIC FOCUS..... 449
Security in the Black Sea Region. Shared challenges, sustainable future Program
CRESCEnt Project
ARMOUR Project
Call for Paper *Romanian Intelligence Studies Review*..... 451

INTELLIGENCE ANALYSIS

EXPLORING UNKNOWN UNKNOWNS IN INTELLIGENCE ANALYSIS

Patrick RUS*

Abstract

Intelligence analysts are confronted always with gaps in the intelligence cycle that limit their understanding, explanation and prediction of phenomena that are outside their subjective and bounded rationality knowledge horizon. When they reach the inflection point in intelligence analysis, they are either inclined to make guesses or estimates that are based on their experiences and cognitive biases. Going far ahead the inflection point, there is the highest level of uncertainty that goes far beyond our capability to understand, explain and predict the phenomena. The highest level of uncertainty can be traced back to concepts such as Thucydides' tyche or Rumsfeld's unknown unknowns. How can we approach and assess this level of uncertainty? Our position paper argues that this level of uncertainty represents the knowledge/ignorance imbalance in our brains. In order to explore the unknown unknowns, we need to determine this imbalance by approaching the processes and mechanisms that generate ignorance in the Leibnizian and Xenopolian manner. This line of inquiry is convergent with the exploration concept that means "action at a distance". Exploration establishes the (mediating) link between intelligence and immediate action on a tight timeline. Historically, in the Roman Empire, exploratores operated at a geographically and temporally distance to detect, check, monitor, prevent, and react in case of unknown unknowns. "Back to the future", intelligence analysts have to be like exploratores and to look at all the possible indications far ahead their immediate knowledge horizon.

Keywords: *cognitive biases*, *exploration; intelligence analysts, knowledge/ ignorance imbalance; unknown unknowns*.

Introduction

One of the main problems in intelligence analysis is that of knowledge gaps that limit our understanding, explanation and prediction of the potential

* President, Security Studies Group, rus.patrick25@gmail.com.

phenomena. Knowledge gaps may arise from our human knowledge limitations or ignorance. These limitations may be determined by our cognitive biases that are embedded in our experiences in the work that direct our observations, decisions and actions. There are four types of errors stated from the ancient times by Roger Bacon that may impede our knowledge: submission to faulty and unworthy authority, influence of custom, popular prejudice and concealment of our own ignorance accompanied by an ostentatious display of our knowledge (INCOSE-LA, 2008). Thus, as humans we may be subject to these types of errors and consequently we are surrounded by our own ignorance.

Due to the increasing complexity of our world, intelligence analysts are confronted more and more with knowledge gaps in the intelligence cycle. Moreover, they are always under external constraints of time, resources and bureaucratic requirements and internally by their own knowledge/ignorance imbalance regarding the unknown phenomena. Intelligence analysts have to respond to growing complexity of data and uncertainty by using their brains connected nowadays with technology in order to prepare the intelligence products. However, technological tools are only mediating processes in their work and hence, they need to approach the phenomena in different ways to formulate the problems and find answers.

Our position paper proposes a different approach that may provide a proper response to the highest level of uncertainty that goes far beyond our capability as intelligence analysts to understand, explain and predict the phenomena involved in intelligence analysis. The highest level of uncertainty can be traced back to concepts such as Thucydides' *tyche* or Donald Rumsfeld's unknown unknowns category of events. This category is defined as a class of ignorance alongside intelligence errors, biases, blind spots, that occur in intelligence analysis.

In order to approach this class of ignorance, namely unknown unknowns, we propose the concept of exploration (*exploration)* as used by Austin and Rankov (1995), as the intervening variable between intelligence analysis and action at operational level. Hence, in the first part of the paper we trace historically the concept of exploration in light of unknown unknowns events. We argue that exploration is a mediating process in the intelligence cycle and it should be included into it in order to manage the classes of ignorance. Finally, we provide few examples from the private intelligence sector, where office investigators are confronted with unknown unknowns in their activity.

Intelligence analysis – exploration – action

Since the ancient times, exploration was a basic human instinct for searching and discovery of knowledge about the world. In "Report on The Exploration" delivered to Moses, we find out about the conditions into an unknown land. Explorers in the Spanish Empire, Elizabethan England, Dutch Empire, and Venice Republic were sent to distant places to discover knowledge about the lands, inhabitants, climatic conditions, trade and so on. They brought home relevant knowledge in the form of maps and records that were used by a small secret segment of people to control and dominate the world in specific periods of time.

Also, private companies such as British East India Company and Dutch East India Company sent explorers to better understand the trade routes and the traders in their operation fields. Exploring unknown lands and the populations was a prerequisite for understanding other cultures and assessing their capabilities.

The Roman Empire was the first that developed exploration units that operated at a distance to detect, check, monitor, prevent, and react in case of unknown unknowns. In the Roman Empire, exploration was only used for field operation units specially trained. Their mission was to investigate in the immediate vicinity the tactical items of intelligence that would affect the implementation of the strategic plan. Moreover, they were used to collect topologically intelligence about the route that may be taken by the army, provide security throughout army movements, search for clues in the enemy camp, check the evidences of hostile activity, prevent the surprises, deep screen within which intelligence could be gathered, continuous monitoring the clues. Exploration is thus the mediating link between intelligence and action, providing operational time and, by constant monitoring the situations, it brings inputs in the intelligence agency's responses.

Theoretically, one of the definitions of exploration is action at a distance. Being a concept from physics, proposed firstly by Leibniz, action at a distance is a means of communication between separated objects that are not locally placed (Hesse, 1955). This type of action is intangible. It can only be grasped by retrodiction that is an operation in the past in order to infer the "most probable cause". Because our knowledge is incomplete, we establish by retrodiction a plausible explanation of the cause of events. Xenopol's approach was exactly in the sense proposed by Leibniz and suggested the retrodiction operation in establishing the "genesis of a phenomenon" (Xenopol, 1906; 1997; Veyne, 1984). His approach is based on a fundamental distinction between repetitive and successive phenomena that comprise different logics.

Our interest is successive phenomena that are fallen in the unknown unknowns category and which require a dynamic logic of clues and evidences and a different probabilistic reasoning.

The distinction made is important in understanding the exploration process, because we are not looking for repetitive phenomena, but for unknown unknowns, that are comprised in successive events. The process of exploration does not start from known unknowns, but from unknown unknowns events in the past and future. Thus, our way of operation as analysts should start by determining our ignorance in relation the phenomena explored. Setting the limits of human knowledge is fundamental in the exploration process. This may be done by establishing constraints on our own judgments regarding a potential situation.

Because the main problem in intelligence is anticipation of future events in a finite time, intelligence analysts are always under pressure and constrained by internal and external factors. Exploration looks far beyond our knowledge horizon are for identifying weak signals or clues that can be monitored constantly. Exploration is based thus on a dynamic logic of clues and evidence followed by assigned probabilistic values on the conjectures proposed regarding the future events and error values on our own judgments vis-à-vis those events (see for example, Kyburg, 1979). Hence, this provides a way to assess the highest level of uncertainty and to admit our own ignorance, by regarding our own judgments errors. The probability values assigned constrain the conjectures proposed within certain intervals. This should be transformed into a probabilistic model that regards the past and future events. Past events should be explored by retrodiction that cover the knowledge gaps and the future events should be assessed by present and future conjectures proposed that are assigned within a certain probability interval.

Intelligence analysis does not have to, the author's knowledge, an approach based on retrodiction operation and does not have a logic based on searching and monitoring clues, gathering and checking evidences. The exploration approach would cover this fundamental gap in the intelligence cycle and it would improve the intelligence fusion process and anticipation. The intelligence fusion process is a stock of knowledge at a time interval and in this process; exploration would keep the constant flow of intelligence updated with all possible indications regarding the threats and risks.

Despite the fact that historically, exploration was used only for field operations, today it is practiced by office investigators that are working in the private intelligence industry. Thus, exploration should be viewed as a practice and a process that has its own purpose, namely to reduce the knowledge/ignorance imbalance in the intelligence analysis.

Exploring unknown unknowns

In intelligence analysis we are not dealing with what we know, but with unknown unknowns, in order to anticipate the intentions, interests and capabilities of enemies or other threats (i.e. African swine fever virus, criminal organized networks, terrorism so on).

The category of unknown unknowns was officially used by Donald H. Rumsfeld in relation with Iraqi weapons of mass destruction in 2002 and it means that we don't know what we don't know (Rumsfeld, 2011). Historically, it can be traced back to the Greek concept of tyche that means a cause of events not governed by laws of nature (Borchert, 2006: 125-130). It can be seen at Xenopol (1906; 1997) in the concept of hazard or elsewhere as chance. Tyche was included in the probability theory by Billingsley (1965:5) that stated that tyche is a point drawn out of space. This point has to be anticipated at a given point in time by the intelligence analysts.

This category is not approached in intelligence analysis properly and this needs further attention. It requires looking at our own ignorance and it involves broad search activity into unknown. We have to look at what we and others don't look; we have to search for clues that are hidden and to anticipate the interests and intentions by exploring the unexplored threats and risks.

We have to state that this category of unknown unknowns is naturally and socially restricted to a small segment of intelligence analysts that understand the `secret world` and have the capability to detect the possible indications and estimate probabilistically the uncertainties.

Unknown unknowns require intelligence analysts that are able to understand and explain the social mechanisms behind phenomena. Not all the analysts have the capability to understand these mechanisms, as not all the scientists in the time of Elizabethan England understood the works of Francis Bacon, Robert Hooke, for example.

Xenopol's approach is best suited here for providing an historical explanation by retrodiction. His approach allows to discover the most probable events in the history and to establish the succession series for anticipating unknown unknowns.

Intelligence analysts as future explorers?

As a work environment based on routine activities, as such within an intelligence agency, it is hard to induce a mental map transformation to intelligence analysts that were trained in a particular way to look at the things, but there are among them analysts that understand the limits and the problems involved in intelligence analysis. Due to the fact that, intelligence

organizations and the analysts that work on daily basis learn extremely hard when they encounter errors in the intelligence process or more serious, intelligence failures, there is a slow process in the transformation of the mental map towards addressing unknown unknowns. There is a possibility to approach the process from the beginning, when new intelligence students are trained and specialized, but this involves an intelligence program in unknown unknowns that is suited for a selected team of analysts that are learning from their ignorance.

Exploring unknown unknowns in the private intelligence realm

In the private intelligence sector, office investigations are everyday encountered with known unknowns and unknown unknowns. The process of investigation is a particular case of exploration. The last category of unknown unknowns is when they have no knowledge at all about the case and throughout the investigation process they discover something that they never encountered before. This will change their mental map by adding a new item of knowledge and reducing the ignorance. However, continuously searching for clues and linking dots between items bring another piece of knowledge and so on. Thus, the process of acquiring new knowledge is from the fountain of our ignorance towards what is outside, in the unexplored world. We can only become better prepared if we constantly monitor the security environment and define the probability parameters and the probability of our judgment errors.

In the private intelligence sector there are also intelligence failures, but the impact is only on a small segment of persons that is responsible for a case or cases. However, the impact of a private intelligence failure affects the reputation of those involved, of the firms, employees, partners and the competitors that may win potential clients. Thus, there is no space for errors. Some of the investigation cases may imply assessing uncertainties at micro (employee, entrepreneur), mezzo (department) or macro (company) level. At micro level, the exploration process is cantered for example on determining the interests that a businessman wants to protect, his potential intentions regarding the strategy and his capabilities. In doing so, we have to search into unknown all the possible items. At the macro level, a case may imply a potential acquisition on the market by a foreign investor and this requires due diligence processes for determining the history, connections of the shareholders and the firms, properties, incomes and other hidden things. In this case, the intelligence report should assess and estimate the risks and uncertainties involved.

Conclusion and perspectives

In this paper we argued for the inclusion of the exploration process into the intelligence cycle in order to approach and assess the highest level of uncertainty that is unknown unknowns. Exploration process is a mediating variable between intelligence analysis and action at operational level that add value to the intelligence cycle. Firstly, by exploration we address our own ignorance regarding what we don't know we don't know in the world. In intelligence analysis, from Sherman Kent to now, we were taught that "Intelligence is Knowledge, Knowledge is Power", but we try to see different and to put it differently as "Ignorance is Power". This means that the process of knowledge starts from what we don't know we don't know, namely our ignorance. Consequently, those who acknowledge their ignorance and step into the unknown unknowns may accumulate power. Furthermore, as historically we saw the biggest intelligence failures (i.e., Pearl Harbor, 9/11) as unknown unknowns, we have to become more aware of our ignorance and to address it.

The exploration process involves a mental map transformation that is very hard to induce into an intelligence agency, because of the routine activities. There are almost no mechanisms for learning within an agency and my ignorance is pushing me to affirm that the intelligence analysts do not know how to learn, except of experience. Learning how to learn is not approached in a theoretical manner and this generates vulnerabilities on long term. Moreover, learning based on experience and unlearning based on a theoretical approach may generate unknown unknowns. This is because of the cognitive biases and blind spots rooted in routine activities.

Thereby, any intelligence process has limits and this may be covered by exploration process in order to reduce the knowledge/ignorance imbalance. An exploration process may complement the intelligence cycle by looking for unknown unknowns, setting the limits of human judgments and finding the error judgments, monitoring clues and gathering evidences, exploring them in depth and breath, providing an enhanced screen of intelligence stock and delivery in operational time that connects the strategic, tactical and operational fields.

Of course, as any concept, exploration has its own limits that are part of the incomplete intelligence system. Some analysts are stating that we cannot anticipate the unknown unknowns and we can only make guesses or approximate the uncertainty in the security environments. Our perspective is that we conceal our ignorance and we are not addressing it in a proper way. Addressing it means to explore the unknown unknowns, to generate actionable intelligence.

References:

1. Austin, N.J.E., and Rankov, N.B. (1995). *Exploratio: Military & Political Intelligence in the Roman World from the Second Punic War to the Battle of Adrianople*. New York: Routledge.

2. Billingsley, P. (1965). *Ergodic Theory and Information*, New York: John Wiley & Sons, Inc.

3. Borchert, M. Donald, (2006), *Encyclopedia of philosophy*, 2nd edition, Thomson Gale.

4. Hesse, Mary B. (1955). "Action at a Distance in Classical Physics". *Isis*, 46 (4): 337-353.

5. INCOSE-LA (2008). "Causes of Error" (or Root Cause Analysis Before We Invented RCA). An Analysis by Roger Bacon. *INCOSE*, 6 (6): 1-2.

6. Kyburg, E. Henry (1979). Tyche and Athena. *Synthese,* 40: 415-438.

7. Rumsfeld, Donald (2011). *Known and Unknown: A Memoir*, New York: Sentinel.

8. Veyne, Paul (1984). *Writing History: Essay on Epistemology*, trans. by Mina Moore Rinvolucri, Middletown, Connecticut: Wesleyan University Press.

9. Xenopol, A.D. (1906). "Cauzalitatea in succesiune". *Analele Academiei Romane*, 28 (7): 531-577.

10. Xenopol, A.D. (1997). *Teoria Istoriei*, translated from French by Olga Zaicik, Bucuresti: Editura Fundatiei Culturale Romane.

CALLING A SPADE, A SPADE: A RETURN TO 'COUNTERESPIONAGE' FROM 'COUNTER-INTELLIGENCE'

Jules J. S. GASPARD*

Abstract

This paper argues that our theorising of 'counter-intelligence' leaves much to be desired. It maintains that in terms of engagement with the concept, current theory lags far behind our understanding of intelligence – which itself has frequently been accused of being 'under-theorised' in definitional debates. By carefully assessing current works on counter-intelligence theory and practice, and interrogating this theorising, I find three flaws that are necessarily in need of being addressed.

First, I argue that previous authors have all attempted to locate the essence of 'counter-intelligence' in its activities and not in its goal. Second, the article demonstrates that the overwhelming majority of scholars who have engaged in setting the boundaries and defining counter-intelligence have worked, or currently work within the US intelligence community. This US intelligence practitioner emphasis in the literature not only undermines the integrity of the concept as it results in mono-cultural understanding but, more profoundly, it has sanitised our understanding of the concept. Thus, lastly, I argue – by exploring contemporary developments in security services – that activities from these state bureaucracies are best defined by a return to 'counterespionage' and a move away from 'counter-intelligence'.

Keywords: *counter-intelligence, counterespionage, intelligence theory, intelligence studies, philosophy of language*.

Countering Intelligence

Our theorising of 'counter-intelligence' leaves much to be desired. In terms of engagement with the concept, current theory lags far behind our understanding of intelligence – which itself has frequently been accused of being 'under-theorised' in definitional debates (Andrew, 2004, pp. 170-184). There are obvious reasons why our knowledge and understanding of 'counter-

* Lecturer in Digital Intelligence, King's College London, jules.gaspard@kcl.ac.uk.

intelligence' is behind other elements frequently associated with intelligence. First and foremost is linguistic – the ordinary treatment of prefixes. An uncritical glance could dismiss counter-intelligence by simply asserting that the hyphen assures the reader that 'counter-intelligence' is simply an attempt to frustrate the attempts of intelligence. In no term containing a hyphen is the second part unconnected to the first; for example: anti-personnel, anti (or counter) – clockwise, counter-force or counter-plot. Common usage of the word 'counter' in ordinary language would further indicate to the reader that counter-intelligence is simply that which counters intelligence; a verb that encapsulates an act in opposition to a noun (in this case intelligence). As such, the prefix and hyphen are relegated in the meaning of the concept – if one has a sure concept of intelligence then they understand what is being countered, thus what counter-intelligence means. All that is left for those who wish to contribute to a literature of counter-intelligence is to describe what efforts can be taken to 'counter' intelligence. Hence, as will be shown below, the literature focuses almost exclusively on methods – the 'vaults mirrors and masks', to borrow the title from one of one of the most popular titles on counter-intelligence (Sims and Gerber, 2009).

What is missing from the literature is engagement with 'counter-intelligence' (perhaps more pragmatically written 'counterintelligence') as a noun, as a unique concept distinct from 'intelligence'. This refers to theorising on counter-intelligence which is not partly or wholly contingent on intelligence. The meta- argument of this paper is for a linguistic turn and a return to counterespionage from counter-intelligence, both in semantics and essence. The paper starts by showing the evolution of counterespionage into counter-intelligence and the problems, both semantic and conceptual, that this has caused. From there the paper goes on to argue that previous authors have all attempted to locate the essence of 'counter-intelligence' in its activities and not in its goal. It argues that is a consequence of all majorities of scholars who have engaged in setting the boundaries and defining counter-intelligence have worked, or currently work within the US intelligence community. This US intelligence practitioner emphasis in the literature not only undermines the integrity of the concept, as it results in mono-cultural understanding but, more profoundly, it has sanitised our understanding of the concept. Thus, in the final section, I argue by exploring contemporary developments in security services that activities from state bureaucracies are best defined by a return to 'counterespionage' and a move away from 'counter-intelligence' with a focus on the aims of counterespionage and not a sanitised focus on means.

The inception and growth of 'Counter-Intelligence'

Counterespionage and counter-intelligence signify the same concept when discussing contemporary developments in security services, but the words' genealogies are distinct. It is best to start at the start, with the etymology of both words. The etymology of a word is important as it teases out root ideas, provides clarity and vivid context for a concept being signified (Donald, 1872, p. V). The etymology of 'intelligence' comes from the Latin word — *Intelligentia, intelligens* — meaning 'communicator of news' or 'one who conveys intelligence' (Donald, 1872, p. 266). Espionage, on the other hand, is from the French *espionnage* meaning 'spying', which is from Middle French *espionner* 'to spy'.[1] *'Espionner '*, in turn, is from mid-thirteenth century French *espier*, meaning 'to watch stealthily' (Donald, 1872, p. 161).

Language obviously has all sorts of uses, but we ordinarily use it to communicate an idea as clearly as possible. This, however, is not its only function; it can also be used to obfuscate. The substitution of 'counter-intelligence' for 'counterespionage' is an example of such euphemistic obfuscation (Donald, 1872, p. 161). The George Bush administration's efforts to retitle 'torture' as 'enhanced interrogation techniques', is a well-known example of deliberately using a more complex term to hide its less pleasant aspects (Cole, 2009).

Obfuscation can also occur in the social sciences when writers attempt to emulate the rigour of the natural-sciences and circumvent the imprecision of ordinary language with unnecessarily complex terminology (Walt, *Foreign Policy*, 15 February, 2013). This is not to say that the employment of sophisticated language does not have a useful purpose. The development of discipline-specific terminology is often vital to explaining new, complex concepts by stipulating exactitude upon terms and making them measurable via experiments or observation. 'Counter-intelligence', however, conveys no extra rigour, extra precision in terms of meaning, no better understanding of the activities it purports to delineate than 'counterespionage'. In fact, counter-intelligence does the opposite – it is (and has been) used by government legislation, security organisations and academics to conceal 'the soft underbelly' of the less scrupulous methods of the concept lurking below the surface. It has also been used to obscure the extent to which surveillance for legitimate security purposes can quickly slide into suspicion against those who do not conform to dominant social or political norm.

[1] Both 'intelligence' and 'espionage' are from the seventeenth century.

Earliest British intelligence files illustrate the all-encompassing nature of the terrain that a concept signified by either counter-intelligence or counterespionage had to unavoidably traverse. In 1921, an MI5 report produced by G. Branch on 'the investigation of espionage', in the preface on 'the experience of M.I.5 from 1909 to 1918', produced a rather pivotal distinction. In the latter years of the First World War, German intelligence sent fewer agents to the United Kingdom for the purpose of 'espionage proper', as the bulk of Britain's armed forces were abroad (The National Archives, KV 1/39, 1921, p. 8.). The experience of MI5 between 1909 and 1918 was that Germany's concept of espionage embraced 'the whole life of the state: naval, military, economic, political and social...' with even 'the conduct and fortune of private citizens of interest to them' (The National Archives, KV 1/39, 1921, p. 7.). They did not only collect information related to military preparedness, but also 'stirred up discontent and strikes' and conducted 'commercial penetration.' (The National Archives, KV 1/39, 1921, p. 7) As such, in understanding what countering 'espionage' was, MI5 needed to cover the same expansive concept of espionage in order to counter it. Here is the salient part of the report: 'its [Germany's] elements are so various and inclusive that in legislation the wider term, "German agent" is now substituted for that of spy, and similarly the expression "Defence Security Intelligence" of larger connotation than "counterespionage" has been adopted to express more adequately the work done by M.I.5.' (The National Archives, KV 1/39, 1921, p. 9) From the early 1920s, terms like 'defence security intelligence' started to come into use, though the explanation offered here was because – ironically – counterespionage failed to capture the alleged breadth of German intrigue within Britain. Counterespionage would remain the dominant terminology to define the activities of secret and security services in English-speaking countries until the run up to the Second World War. From the mid-1930s onwards, however, counter-intelligence would begin its precipitous rise and eventually over-take counterespionage, which simultaneously began its slow decline – leaving us where we are today, where counter-intelligence reigns supreme.

This trend is not just observable from impressionistic anecdotal engagements with the files and the literature, but also through gigantic leaps in search engine technology that enable the scanning and registering of impressions of the use of specific terms. *Google Books Ngram Viewer* – an online search engine that charts frequencies of any set of comma-delimited search strings using a yearly count of n-grams found in sources printed

between 1500 and 2008 – demonstrates unequivocally the substitution of 'counterespionage' with 'counter-intelligence' since the 1920s.[2]

The adoption of 'counter-intelligence' instead of 'counterespionage' over time would have been a rational shift if it reflected a desire to encompass the broadening of the German activities within the concept identified in the MI5 report in 1921. However, 'counter-intelligence' – much like the word 'intelligence' – is preferred by governments the world over for the clean, clinical veneer it paints over the activity. The word semantically projects a sense of 'communicator of news' and not 'watching stealthy', as the etymology of both the words above shows. It is a clever trickery of language aimed at sanitising the business by illuminating activities that go along with the concept, while detaching it from the *espion* – the spy. As the next section will show, counter-intelligence theorising within the literature is similarly purged of its dubious motives, means and ends; whilst most frequently being analysed during wars and against foreign states, conferring a cloak of legitimacy over the activities.[3] However, despite the seemingly neutral framing, counter-intelligence is more than that.

Counter-Intelligence in the literature

Ordinarily Scholars are typically the individuals best placed to highlight the discrepancies between jargon and terminology, and comprehensive and partial theorising; as they are the individuals with the best command of the discipline. However, when it comes to understanding counter-intelligence, the overwhelming majority of those who have contributed to the debate on the theorising of the term have been former or current practitioners. As such, they are the least likely to highlight discrepancies, as they have a strong interest in projecting an image of 'counter-intelligence' that confers legitimacy and proportionality, as they have (in some cases still do) partaken in it.[4] The term 'counter-intelligence' adds

[2] An 'n-gram' is a contiguous sequence of n items from a given sequence of text or speech. The items can be phonemes, syllables, letters, words or base pairs according to the application. The n-grams typically are collected from a text or speech corpus. In the case of *Google Books Ngram Viewer* it is scanned books, newspapers, periodicals and journals available on *Google Books*. Even with the criticism of the software, the trends both ways are pronounced enough to demonstrate a switch out of 'counterespionage' and switch in of 'counter-intelligence.' See: *Google Books Ngram Viewer*, words searched 'counter-intelligence' and 'counterespionage' and variations of spellings, available from: https://books.google.com/ngrams.

[3] Unless within the studies of intelligence, the writers are talking about Soviet counterespionage.

[4] I highlight in text and footnotes when a scholar has worked in the intelligence community throughout the remainder of this exploration on definitions.

nothing to counterespionage – which was the term used in the nineteenth and most of the early twentieth century. Not only does the term deceive, but the significant body of writing claiming to theorise counter-intelligence is limited and written almost exclusively by former intelligence officers, leaving only a partial understanding of the concept at best.

Quite apart from the ambiguities in our understanding as a result of the aforementioned semantic obfuscation, our knowledge of counter-intelligence is less complete than our knowledge of other components of intelligence for other reasons. There are three primary factors at work here. First, much of the recent theorising on intelligence generally within the literature has almost entirely ignored 'counter-intelligence'.[5]

Second, as we have already seen, counter-intelligence is in a 'semantic rut' (Geschwind, 1963, p. 25). In 1963, C.N. Geschwind identified in the CIA's journal *Studies in Intelligence*, that '"intelligence" as the root of "counterintelligence" distorted thinking on the term, noting 'it is no exaggeration to say that the word "counterintelligence" has become one of the most dangerously misleading in our language because it enshrines the concept that in counterintelligence we are countering the operations of a hostile intelligence organization.' (Geschwind, 1963, p. 25) His reflection is still as accurate in the twenty-first century. In the US (where the majority in the discipline broadly known as 'Intelligence Studies' define intelligence as timely, good, relevant information to help decision-makers formulate sound policy) counter-intelligence is simply the thwarting of those same endeavours by foreign intelligence services.[6]

---

[5] See, for example, Richard Betts, *Enemies of Intelligence* (New York, NY: Columbia University Press, 2007); Gregory Treverton et al., *Toward a Theory of Intelligence*: *A Workshop Report* (Arlington, VA: Rand Corporation, 2006); Len Scott and Peter Jackson, 'The Study of Intelligence in Theory and Practice', *Intelligence and National Security*, Vol. 19, No. 2 (2004), pp. 139–69; Loch Johnson, 'Preface to a Theory of Strategic Intelligence', *International Journal of Intelligence and Counter-intelligence*, Vol. 16, No. 4 (2003), pp. 638–63; Loch Johnson, 'Bricks and Mortar for a Theory of Intelligence', *Comparative Strategy*, Vol. 22, No. 1 (2003), pp. 1–28; Michael Warner, 'Wanted: A Definition of "Intelligence"', *Studies in Intelligence*, Vol. 46, No. 3 (2002), pp. 15–22; David Kahn, 'An Historical Theory of Intelligence', *Intelligence and National Security*, Vol. 16, No. 3 (2001), pp. 79–92; Stafford Thomas, 'A Political Theory of the CIA', *International Journal of Intelligence and Counter-intelligence*, Vol. 11, No. 1 (1998), pp. 57–72; and Michael Handel, 'The Politics of Intelligence', *Intelligence and National Security*, Vol. 2, No. 4 (1987), pp. 5–46.

[6] See the following for broad definitions of intelligence: Frederick L. Wettering, 'Counterintelligence: The Broken Triad', *International Journal of Intelligence and Counterintelligence*, Vol. 13, No. 3 (2000), pp. 265-300; Roy Godson, *Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence* (Washington, DC: Pergamon-Brassey's, 1995), p. 2; Warner, 'Wanted: A Definition', pp. 20-22; Jennifer Sims, 'The Theory and Philosophy of Intelligence', in Robert Dover, Michael S. Goodman and Claudia Hillebrand (eds.), *Routledge*

Lastly, and proportionately the weightiest explanation of the three, is connected to the core of counter-intelligence. As the countering of foreign intelligence takes place within the jurisdiction of the state, it intersects with citizens who have constitutional rights – rights that (in the US) severely curtail the repertoire of tools a permanent federal bureaucracy mandated to perform counter-intelligence would otherwise exploit. Connected to this quandary is the almost exclusive theorising on counter-intelligence by individuals currently or previously employed within the US intelligence community. With respect to theorising on the subject, the preponderance of engagement by intelligence officers has skewed our understanding of counter-intelligence. Since the early 1960s, research has been undertaken that sketches out a theory of counter-intelligence which focuses on legitimate methods, a focus on agents from foreign states during war and expresses a disregard for the *purpose* – the overall objective of all counter-intelligence operations.

Occasionally, counterespionage is split into two branches: defensive measures (efforts taken to prevent a rival's espionage) and offensive measures (deception activities an intelligence organisation may take in order to purposely mislead other rival intelligence organisations).[7] Unsurprisingly, theorising by officials or former officials has focused on either 'passive', 'reactive' or 'defensive' activities – keeping sensitive information in vaults and behind firewalls, protecting state secrets by maintaining good levels of personnel security, conducting background investigations and reinvestigations, and observance of the 'need to know' principle.

The less theorised component is frequently described as 'offensive'. When discussing offensive measures, counter-intelligence takes the form of recruiting double agents (moles) to learn the identity, methods and operations of the intelligence service from 'their' spies. It endeavours to preoccupy or distract a rival state's counter-intelligence apparatus with the goal of achieving 'strategic deception', by the double agent(s) feeding a steady stream of disinformation and by manipulation. However, offensive measures are

Companion to Intelligence Studies (London: Routledge, 2014); David Kahn, 'An Historical Theory of Intelligence', *Intelligence and National Security*, Vol. 16, No. 3 (2001), p. 79.

[7] See, for example: Hank Prunckun, *Counterintelligence Theory and Practice* (Lanham, MD: Rowman & Littlefield, 2012); James M. Olson, 'The Ten Commandments of Counterintelligence', *Studies in Intelligence*, Vol. 45, No. 3 (2001), pp. 81–87; David Tucker, *The End of Intelligence: Espionage and State Power in the Information Age* (Stanford, CA: Stanford University Press, 2014) p. 74; William R. Johnson, *Thwarting Enemies at Home and Abroad: How to Be A Counterintelligence Officer*, 2nd ed. (Washington, DC: Georgetown University Press, 2009), pp. 1-4, though Johnson, like many of the authors cited in this section, thinks of counterespionage as being a sub-section of counter-intelligence. It is worth adding that Tucker worked within Department of Defence, Johnson within the CIA.

usually broached in defensive terms, controlled and clean operations that are frequently framed against agents of foreign powers, with little to no mention of how counter-intelligence intersects with the lives of a state's citizens. Nor are there mentions of offensive measures – agents provocateurs, blackmail, informants, intimidation, subversion and deportation – which are rarely included in the theorising of the institutional arsenal historically of western security services.

Not all attempts to understand counter-intelligence have focused on this bipartite framework. The majority of counter-intelligence theorists' classifications of counter-intelligence have been either on a tripartite or quadripartite basis. Indeed, one author has approached counter-intelligence by breaking it down into a quintipartite (Redmond, 2010, pp. 537-554.).[8] Though the conceptualisation proliferates, the focus on outside forces continues. Michelle Van Cleave – who served as the first National Counter-intelligence Executive under President George W. Bush – notes the 'signature purpose of counterintelligence' as to 'confront and engage the adversary' (Van Cleave, 2007, pp. 1-15). Across her three major contributions, she conceptually broke counter-intelligence down into four components: identifying (spies); assessing (analysis); neutralising and exploiting (offensive) (Van Cleave, 2007a, pp. 5-11; Van Cleave, 2013, p. 58).[9]

George Kalanis and Leonard McCoy also split counter-intelligence into four sections (penetrating hostile intelligence services, research and information collection on hostile intelligence services, disrupting and neutralising hostile intelligence services and assessing the bona-fides of defectors), a typology that is not dissimilar to that of Van Cleave (Kalaris, McCoy, 1988, pp. 179–187). Moreover, like the former-Counter-intelligence Executive, the pair – both former CIA counter-intelligence officers – focus on 'hostile intelligence services', not citizens whose crimes would not be considered espionage, but potentially treason. In addition, no mention is made of the use of belligerent methods, attributed only to hostile intelligence (Richelson, 1989, p. 318).[10] Christopher Felix – a pseudonym for another intelligence officer, James McCargar, who served in the CIA during the early

[8] Paul Redmond is yet another counter-intelligence officer, indeed an extremely senior one. At the time of his retirement he was head of Counterintelligence at the CIA. His five parts are: (1) as Counterespionage; (2) as Asset Validation; (3) as Disinformation Operations; (4) as Operational Tradecraft; (5) as the Recruitment and Running of Counterintelligence Sources.

[9] Though in the latter article she breaks up counter-intelligence differently from in her earlier *Counterintelligence and National Security*.

[10] Jeffrey Richelson also offers four functions in the practice of counter-intelligence virtually identical to Kalaris and McCoy.

Cold War, also defines counter-intelligence in four parts (Felix, 2001, p. 126; Stout, 2004, pp. 69-82). In 1989, a further group of counter-intelligence experts met and also defined counter-intelligence in terms of organisational activity, functionally splitting counter-intelligence into four similar groups to those above (Graffenreid, 1989), p. 3).

Jennifer Sims and Burton Gerber – two more individuals who have contributed to theorising on counter-intelligence from within the US intelligence community, also define counter-intelligence based on four activities: 'Decision makers matching wits with an adversary want intelligence – good, relevant information to help them win. Intelligence can gain these advantages through directed research and analysis, agile collection, and the timely use of guile and theft. Counterintelligence is the art and practice of defeating these endeavours. Its purpose is the same as that of positive intelligence – to gain advantage – but it does so by *exploiting*, *disrupting*, *denying*, or *manipulating* (my own italics) the intelligence activities of others.' (Sims and Gerber, 2009).[11] Uniquely, Sims and Gerber provide a purpose, to gain advantage, but the purpose is sufficiently broad to be almost meaningless.

Equally, counter-intelligence theorists' classifications of counter-intelligence have been developed on a tripartite basis, with a focus on mechanisms and disregard for purpose and non-foreigners. The first to expound such a typology was another former CIA officer, Charles V. Cate. (Cate, 1958, pp. 87-92; Wasemiller, 1969, pp. 9-24)[12] Building upon Sherman Kent's tripartite framework for considering intelligence matters, the author discusses counter-intelligence as a confluence of knowledge, activity and organisation (Kent, 1949, p. IX). Arthur A. Zuewle – a former Soviet analyst from the Defense Intelligence Agency – also breaks down counter-intelligence into three constituent parts with two of those – 'aggressive' and 'defensive' – mirroring the classical duel taxonomy. He adds 'preventative' to the mix, segmenting defensive measures, mirroring Soviet ideas of prophylactic measures to some degree (Zuehlke, 1980). Along the same lines, Frederick L. Wettering – another retired CIA officer – conceptualises counter-intelligence as: 'protecting secrets', 'catching Americans that spy for foreign intelligence services', and 'frustrating attempts by foreign intelligence services'.

[11] Sims served as Deputy Assistant Secretary of State for Intelligence Coordination and as the Department of State's first coordinator for intelligence resources and planning. She has also served on the staff of the Senate Select Committee on Intelligence. Gerber served for thirty-nine years as an operations officer in the CIA.

[12] Soon after, A.C. Wasemiller also defined counter-intelligence three ways: as an activity (consisting of counterespionage and security) and a product (reliable information about enemies who use stealth to 'attack' the state).

(Wettering, 2000) Roy Godson strikes a similar chord, defining counter-intelligence as a state's effort 'to protect their secrets, prevent themselves from being manipulated, and (sometimes) to exploit the intelligence activities of others for their own benefit'. (Godson, 1995, p. 2)

Godson, who served on the President's Foreign Intelligence Advisory Board under Ronald Reagan, sagaciously observed in the same book that most writing fails to include not just counter-intelligence but covert action as important 'elements' of intelligence' (Godson, 1995, p. 2). Godson, though not an intelligence officer, was a consummate Washington insider during the Reagan era whose general thesis was that these clandestine arts would be important tools of statecraft in the post-Cold War World. Precisely because he was an influential advocate of the best counter-intelligence constituting an 'offensive defence', his 1995 book highlights the classic myopia within the theorising on intelligence broadly; it demonstrates that under-theorising, combined with popular misconceptions, has resulted in counter-intelligence being regarded as a 'dirty tricks' (Godson, 1995, p. 2). His comments represent an illustration of the remarkable gap between all the sanitised theorising I have considered thus far in this section and a more grounded historical perception of counter-intelligence, which is missing.

Like Godson, John Ehrman – another former-CIA officer who specialised in counter-intelligence – provides a taut definition: 'Counter-intelligence is the study of the organization and behaviour of the intelligence services of foreign states and entities, and the application of the resulting knowledge.' (Ehrman, 2009, pp. 5-20) However, his definition does not fit well with the three types of counter-intelligence operations he identified in his article as the revolve around activities as oppose to process and products: (1) Classic penetration: an officer from a rival service is recruited and provided information from within; (2) Double agents: someone who appears to be working for one intelligence service but in reality is controlled by another and (3) Surveillance by area: through access to agents or physical and technical surveillance to uncover activation and contacts on an enemy service. (Ehrman, 2009, pp. 5-20)

There is a crucial observation we can draw from this section: that everyone that has contributed to a body of literature on counter-intelligence has at some point in their career worked within, or in concert with, the US counter-intelligence community, many within security sections of the CIA. From all the above semi-practitioners/ semi-theorist we have several key – sometimes overlapping – methods and concepts that continually recur; which to borrow a phrase from one of the articles, I would call the classic 'anatomy of counter-intelligence' (Wasemiller, 1969, p. 9):

(1) Being offensive;
(2) Is both an activity and a product?
(3) Entails covert/overt penetration;
(4) Involves double agents and catching spies;
(5) Requires extensive surveillance;
(6) Aims at disrupting and neutralising rival intelligence agencies;
(7) Seeks to protect secrets by *various* means. (Jelen, 1991, pp. 381-399.)[13]

These mutually combined components (which are not exclusively or mutually/jointly sufficient) make up the boundaries of what these authors considered counter-intelligence. As in the next section I endeavour to move beyond them, going forward I will consider them collectively as 'classic counter-intelligence'. The list of characteristics is sanitised and narrow, and avoids regrettable episodes and unsavoury methods in the history and use of counter-intelligence. Chapters in history where the intelligence community has not been used against a rival intelligence service, but rather against one's own citizens, tend to be overlooked.

The various theories considered above are also often disconnected from legislation and conceptions of what it means to be 'disloyal', an 'enemy', 'spy' or 'traitor'. They are equally disconnected from the earliest history of counterespionage, before the Second World War, or what counter-intelligence would mean in a non-state context. Most bizarrely, few provide an 'end' to their list of 'means' outside of the successful completion of the operation for the sake of the operation. In other words, the conception of this subject is remarkably tactical and often lacks strategic context. Counter-intelligence is taken to be a self-evident good and is rarely considered through a critical lens.

A return to 'Counterespionage'

Accordingly, I argue for a return to counterespionage. For an adoption of a much broader and more intuitive stance on the essence of counterespionage, free from the constrained path of the above authors who have so far contributed to the 'theories of counter-intelligence' debate. Instead, a new old term – counterespionage – needs to be deployed that semantically distinguishes itself from the above activist practitioners/

[13] Jelen – a former Director of Operations Security at the National Security Agency – provides an interesting overview of counter-intelligence, though ventures no theory of his own. In this respect he is much like H.H.A. Cooper and Lawrence J. Redlinger, *Catching Spies: Principles and Practice of Counterespionage* (Boulder, CO: Paladin, 1988), p. X.

academics whilst reincorporating the sanctioned with the unsanctioned components of the concept.

Although some authors, like George F. Jelen and William R. Johnson, have thought of counterespionage in narrower terms than (even sometimes as a sub-category of) counter-intelligence, I wish to suggest that the former term better encapsulates the essence of the activities (Jelen, 1991, pp. 381-383; and Johnson, 2009, pp. 1-4). On the one hand, the word 'intelligence', is suggestive of a civilised and justifiable activity that a state undertakes to gain knowledge of the world around them in order to protect the citizen. On the other hand, the word 'espionage', signifies something rather more dastardly, it conveys concealment, subterfuge and/or deceit. It is more than just the gathering of information presumably for the purpose of better informing policy. The two activities – counter-intelligence and counterespionage – are conceptually, and in terms of their etymology, extremely close. One, however, conjures up images in the mind of practices uncivilised; where the other does not. It is the difference between 'torture' and 'enhanced interrogation techniques'.

Theories of counter-intelligence are sanitised, and like the literature on counterespionage, bear little resemblance to the reality of the historical record outside of war. This representational problem however, is not entirely unexpected. If the history and theorising of a discipline are dominated by current and former practitioners, it will not be close to neutral in its approach. Returning once again to the analogy above, it would be akin to a history of torture in America being written by current and former interrogators and jailers from Guantanamo Bay.

Much of the theorising discussed above emphasises 'foreign enemies' (often a code for Soviets), protecting secrets, surveillance and stealing secrets. It is a classical Cold War understanding of counter-intelligence. It fails to talk about supporters of, for example, communism who undertake some of the same activities of Soviet spies but are in fact Americans taking no orders from Moscow. It also fails to account for those on the level of abstraction below; those individuals who do not steal secrets or sow seeds of discontent but provide the material safe-haven for those who do. Or the level of abstraction below that; those who do not even provide a material safe-haven but support the same communistic ends. Their crime is in thought, not in deed, but the history of counterespionage is littered with examples of individuals who have been persecuted for holding opinions that challenged the dominant status quo. That is the real essence of counterespionage. It is concerned with protecting the predominant political social order from various threats, and is not selective in terms of the various offensive and defensive measures it employs.

Substantial theorising within the classic counter-intelligence literature has focused on methods (or activities) – the means – but the ends seem to be simplified, focusing largely on the prevention of intelligence collection by a foe. Not only are less genteel methods side-lined – including agent provocateurs, blackmail, informants, intimidation, subversion, deportation, group infiltration, smear campaigns and integration – but a focus on the means is wrong headed; as the methods are of secondary importance to the goals. Counterespionage is best understood by its *aims*, which are always systematic means delay, frustrate and suppress preliminary stages of organisation before more advanced forms of 'revolutionary radicalism' can develop (Chomsky, 1999, p. 303). It 'counters' these threats through the maintenance and utilisation of activities not ordinarily associated with law enforcement or the army. But so often counterespionage simply concerns itself with the activities of awkward citizens who annoy the state.

Once you analyse counterespionage by its aim – discouraging the fermentation and influence of hostile ideologies – it increases the scope of moments in history that would be considered relevant to an understanding of counterespionage. It opens counterespionage to the unpleasant methods listed above, as opposed to being restricted by the arbitrary lists suggested in most of the previous theorising. It also opens theorising to include the role of the private sector, which has previously been shut out of almost all generalised conceptions which focus on states in the international system.

A definition based on aims also gives us a more complete *critical* account of counterespionage, as it does not just focus on threats to the nature of the state during wartime, but threats from jihadist, organised labour, anarchists and other movements that emanate domestically and challenge the prevailing ideological paradigms. It incorporates countersubversion, counter-conspiracy and – to borrow the wording from the UK Security Service Act – the '…protection of national security against threats from espionage, terrorism and sabotage from the activities of foreign powers and from activities intended to overthrow or undermine parliamentary democracy by political industrial or violent means.' (United Kingdom, *The Security Service Act 1989* (c 5), § 1(a) and (b))

Conclusion

Counterespionage has no meaning without dialectic. Without acknowledgement of a process of societal evolution within the literature on the concept, counterespionage has no deeper meaning. Understood extrinsically, as currently in the literature, counterespionage is relegated to be

understood like a fork (which can only derive purpose through human action). An understanding of counterespionage through human use only not does further our understanding of the concept but ultimately masks it. Counterespionage can only be understood teleological – through engagement with its end goal.

Other than arguing for a fundamental rethink on the theorising of counterespionage, this paper calls forward three other substantive claims. First, that the literature needs a broader basis of contributors, preferably those who are not American and not from the intelligence community. That along with different voices a more sophisticated appraisal of both the history and concept that engages with the counterespionage from an interdisciplinary footing needs to take place. And lastly, that the word 'Counterespionage' ought to make a return at the cost of the corrosion of Counter-Intelligence. This linguistic reversal is not just necessary to avoid obfuscation and equivocation. More importantly, if words are not used correctly, language is not in accordance with the truth of things and wisdom cannot follow. This was true when Confucius uttered it first 475 BC and it is still true today.

References:

1. Andrew, Christopher, (2004), 'Intelligence, International Relations and 'Under-theorisation', in *Intelligence and National Security*, Vol. 19, No. 2.

2. Betts, Richard, (2017), *Enemies of Intelligence*, New York, NY: Columbia University Press.

3. Cate, Charles V., (1958), 'Counterintelligence for National Security', *Studies in Intelligence,* Vol. 2, No. 4.

4. Chomsky, Noam, (1999), 'Domestic Terrorism: Notes on the State System of Oppression', *New Political Science*, Vol. 21, No. 3.

5. Cole, David (ed.), (2009), *The Torture Memos: Rationalizing the Unthinkable*, New York, NY: The New Press.

6. Cooper, H.H.A., Redlinger, Lawrence J., (1988), *Catching Spies: Principles and Practice of Counterespionage*, Boulder, CO: Paladin.

7. Donald, James (ed.), (1872), *Chamber's Etymological Dictionary of the English Language,* Edinburgh: W. & R. Chambers.

8. Ehrman, John, (2009), 'Toward a Theory of CI: What are We Talking about When We Talk about Counterintelligence?' *Studies in Intelligence,* Vol. 53, No. 2, pp. 5-20.

9. Felix, Christopher [James McCargar], (2001), *A Short Course in the Secret War,* 4th ed., Lanham, MD: Madison Books.

10. Geschwind, C.N., (1963), Wanted: An Integrated Counter-intelligence, *Studies in Intelligence,* Vol. 7, No. 3.

11. Godson, Roy, (1995), *Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence*, Washington, DC: Pergamon-Brassey's.

12. Graffenreid, Kenneth E. de, (1989), *Report on a Conference of Security, Counterintelligence, and Strategic Experts on Counterintelligence and Security Requirements for National Strategy*, Washington, DC: National Strategy Information Center, Inc., and Strategic Capabilities Assessment Center.

13. Handel, Michael, (1987), 'The Politics of Intelligence', *Intelligence and National Security*, Vol. 2, No. 4, pp. 5–46.

14. Jelen, George F., (1991), 'The Defensive Disciplines of Intelligence', *International Journal of Intelligence and Counterintelligence,* Vol. 5, No. 4 (1991), pp. 381-399.

15. Johnson, Loch, (2003), 'Preface to a Theory of Strategic Intelligence', *International Journal of Intelligence and Counter-intelligence,* Vol. 16, No. 4, pp. 638–63.

16. Johnson, Loch, (2003a), 'Bricks and Mortar for a Theory of Intelligence', *Comparative Strategy*, Vol. 22, No. 1, pp. 1–28.

17. Johnson, William R., (2009), *Thwarting Enemies at Home and Abroad: How to Be A Counterintelligence Officer*, 2nd ed., Washington, DC: Georgetown University Press.

18. Kahn, David, (2001), 'An Historical Theory of Intelligence', *Intelligence and National Security,* Vol. 16, No. 3.

19. Kalaris, George, McCoy, Leonard, (1988), 'Counterintelligence for the 1990s', *International Journal of Intelligence and Counterintelligence*, Vol. 2, No. 2, pp. 179–187.

20. Kent, Sherman, (1949), *Strategic Intelligence*, Princeton, NJ: Princeton University Press.

21. Olson, James M., (2001), 'The Ten Commandments of Counterintelligence', *Studies in Intelligence*, Vol. 45, No. 3, pp. 81–87.

22. Prunckun, Hank, (2012), *Counterintelligence Theory and Practice*, Lanham, MD: Rowman & Littlefield.

23. Redmond, Paul, (2010), 'The Challenges of Counterintelligence', in Loch Johnson (ed.), *The Oxford Handbook of National Security Intelligence*, New York, NY: Oxford University Press, pp. 537-554.

24. Richelson, Jeffrey T., (1989), *The U.S. Intelligence Community*, 2nd ed., Cambridge, MS: Ballinger Publishing.

25. Scott, Len, Jackson, Peter, (2004), 'The Study of Intelligence in Theory and Practice', *Intelligence and National Security*, Vol. 19, No. 2, pp. 139–69.

26. Sims, Jennifer, Gerber, Burton, (eds.), (2009), *Vaults, Mirrors, and Masks: Rediscovering U.S. Counterintelligence*, Washington, DC: Georgetown University Press.

27. Sims, Jennifer, (2014), 'The Theory and Philosophy of Intelligence', in Robert Dover, Michael S. Goodman and Claudia Hillebrand (eds.), *Routledge Companion to Intelligence Studies*, London: Routledge.

28. Stout, Mark, (2004), 'The Pond: Running Agents for State, War, and the CIA: The Hazards of Private Spy Operations', *Studies in Intelligence*, Vol. 48, No. 3, pp. 69-82.

29. The National Archives, KV 1/39, *The Experience of M.I.5 from 1909 to 1918*, 1921.

30. Thomas, Stafford, (1998), 'A Political Theory of the CIA', *International Journal of Intelligence and Counter-intelligence*, Vol. 11, No. 1, pp. 57–72.

31. Treverton, Gregory et al., (2006), *Toward a Theory of Intelligence: A Workshop Report*, Arlington, VA: Rand Corporation.

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

33. United Kingdom, *The Security Service Act 1989* (c 5), § 1 (a) and (b).

34. Van Cleave, Michelle, (2007), 'Strategic Counterintelligence: What is it, and What Should We Do About it?', *Studies in Intelligence*, Vol. 51, No. 2, pp. 1-15.

35. Van Cleave, Michelle, (2007a), *Counterintelligence and National Security*, Washington, DC: National Defence University Press, pp. 5-11.

36. Van Cleave, Michelle, (2013), 'What Is Counterintelligence? A Guide to Thinking and Teaching about CI', in Peter C. Oleson (ed.), The Guide to the Study of Intelligence, Part 7, *Intelligencer*, Vol. 20, No. 2, p. 58.

37. Walt, Stephen M., (February, 15, 2013), 'On Writing Well', *Foreign Policy*, accessible on <http://foreignpolicy.com/2013/02/15/on-writing-well/.

38. Warner, Michael, (2002), 'Wanted: A Definition of "Intelligence"', *Studies in Intelligence*, Vol. 46, No. 3, pp. 15–22.

39. Wasemiller, A.C., (1969), 'The Anatomy of Counterintelligence', *Studies in Intelligence*, Vol. 13, No. 1, pp. 9-24.

40. Wettering, Frederick L., (2000), 'Counterintelligence: The Broken Triad', *International Journal of Intelligence and Counterintelligence*, Vol. 13, No. 3, pp. 265-300.

41. Zuehlke, Arthur A., (1980), 'What is Counterintelligence?' in Roy S. Godson (ed.), *Intelligence Requirements for the 1980s: Counterintelligence*, Washington DC: National Strategy Information Centre.

OPEN SOURCE INTELLIGENCE (OSINT)

FEATURES OF CHINESE INTELLIGENCE SYSTEM: EXPERIMENTING WITH METAKNOWLEDGE

Mihaela BERBEC*

Abstract

For practitioners and scholars of intelligence alike, referring to the Chinese intelligence system remains a defying task. Until recently, most studies dedicated to China's intelligence research approached the subject from its institutional viewpoint, with a focus on the structure and function of Chinese intelligence services and the immediate relation with the political apparatus (Greenberg, 2007; Mattis, 2012; Inkster, 2013). Relevant for prediction purposes, as well as for the epistemology of the domain, the state of information science research in China should offer clues about the dynamics between politics, science, and the networked framework which facilitates information sharing for national advance and security goals. Along these lines, the development of a paradigm cantered on native intelligence perspectives will readily be possible. Thus, I argue that the Chinese intelligence system remains, with the exception of its secretive apparatus, institutionally and conceptually undefined. However, there are clues in acknowledging experimentation policies from the central government (Bell, 2016) aimed at knitting a native intelligence system, starting with the political support for research concerning metaknowledge.

Keywords: *Chinese intelligence system, Chinese political system, information science, intelligence, metaknowledge*.

Introduction

Lately positioned as major hub in international networks, China seems to take an original stand concerning the use of knowledge to enhance national security policies, and western researches are rapidly concerned with theoretical framing of those strategic moves, that may or may not touch other

* Postdoctoral fellow, at Wuhan University of Technology, China mihaela.berbec@gmail.com.

national security interests in the future. Even outside a realist perspective, the importance of understanding China's relation with the knowledge revolution represents an innovative step for intelligence research.

For some time now, scholars in intelligence research proceed with caution when approaching the topic of intelligence applied to the Chinese security system. This situation is due in part to the opacity of the Chinese governmental policies, but also to a recently discovered gap in understanding Chinese cultural specificity, which could be attributed to its political and social features, combined with its accelerated pace in cyberspace innovations. Therefore, news of experiments conducted in information science laboratories are likely to originate from the Chinese state media, announcing breakthroughs in technological advance.

In the public sphere, the Chinese government publicizes all its technological efforts meant to improve social development policies, along with its longstanding priority in preserving social security and the legitimacy of the ruling party. Statehood in China is assimilated with the communist party ontology. Moreover, the Chinese state security guidelines are contained in the Constitution[1] and the National Intelligence Lawof the People's Republic of China and should be considered the basis for understanding the meaning of security as conceived by the national government.

Therefore, Chinese intelligence services are to be analysed differently than their western counterparts (Greenberg, 2007; Mattis, 2012), seen that the way they operate is different in a practical sense. The sources of its development must be found somewhere else, in another developmental logic. There is a native straight-line dynamic between Chinese politics and science goals, which is confirmed by the network theories advanced in the latest decade in the western literature referring to governance models and social theories. In the case of China as a state, and particularly concerning the Chinese intelligence networks, there is a profound practical meaning of the networking which is applied at all levels of governance, which in turn have as purpose to inspire social networking practices for the benefit of the state.

As follows, intelligence statecraft of Chinese sources is a complex entanglement between politics, policy, security purposes, normative sources to power and social behaviour, all these supported by a communication network meant at facilitating control from the central government. As such, the following research endeavour is meant to address the meaning of

[1] The Constitution was enacted in 1982, with five amendments, 1988, 1993, 1999, 2004, and 2018.

intelligence as the craft of intelligence, a system which should be understood as not only in the way it treats knowledge as end-product, but also as the result of metaknowledge.

An important number of scholars have emphasized the existence of experimental policies, which include by default characteristics related to metaknowledge. The role of metaknowledge became clear along with the 'big data' revolution, when gathering knowledge about a topic remained insufficient for the purposes of arriving to a coherent solution. In China, this phenomenon is augmented by the realization that collecting data in a systematic and global manner will create analytical problems in the future, specifically in respects to state security. Simultaneously with the fast innovations regarding metaknowledge processes and application, the academia receives governmental financial incentives to frame in a theory the uniqueness of the Chinese political system and the advances made in securing its population.

Thus, I argue that the Chinese intelligence system remains, with the exception of its secretive apparatus, institutionally and conceptually undefined. However, there are clues in acknowledging experimentation policies from the central government aimed at knitting a native intelligence system, starting with the political support for research concerning metaknowledge.

In the following pages, I will address the subject of the relation between intelligence and metaknowledge, followed by an account of China's experimental policies, and finally, the clues linking Chinese intelligence statecraft with metaknowledge production.

Metaknowledge and Intelligence

The Kentian meaning of the intelligence process is a historical product. Relevant, timely, accurate information for strategic decision-making is what intelligence represents for practitioners of statecraft intelligence, as well as for intelligence scholars. The concept of national security defines almost fully the intelligence practice inside national structures and is inevitably implying not only the existence of an enemy or a competitor, but also the fact that in relation with oneself, there are only enemies and/or competitors inside a system. The consistent result of this perspective is that intelligence is unable to become overarching in problem-solving, and consistently recurs to the adaptation argument – secrecy, confidentiality, etc., whenever there is the

likelihood of exchange between intelligence practitioners and intelligence scholars.

Along with the increase in complexity of the contemporary intelligence research field, all-known as the big data revolution, intelligence studies are characterized by a phenomenon of branching. On one hand, there is an integration process of interconnected disciplines and methods into a broad theoretical framework, which aims at the creation of an intelligence paradigm. On the other hand, there is a branching process, referring to the creation or resurgence of analysis methods and applications in certain domains, specialized and independent, however having a supporting role for all levels' intelligence. Bridging these two sources is the aim of intelligence for state security.

Intelligence research must remain permanently attached to intelligence practice, where the communities of practice have been implemented or are on their way to become part of the mainstream institutional framework. The recurrence of the topic of bringing together intelligence academics and intelligence practitioners shows there are several issues resulting either from communication or from adaptive issues. More explicitly, the two camps are unable to exchange knowledge, due to creating knowledge based on different criteria and in specific workflows, or they are reluctant in exchanging knowledge due to different value marker assigned to a specific piece of knowledge.

In the first process, there are some priorities concerning processes of definition and meaning in relation with the term security, the taxonomy of the intelligence domain, and the relation with a cosmopolitan version of human and values, a critical part of the paradigmatic build-up. At this point, metaknowledge is generated from analytical processes of high-end priority, strategic intelligence for national or international cooperation security demands.

The last process is characterized to a lesser extent by defining the limits of the field and assigns a higher importance to diversification of methods of collecting, selecting, analysing, managing, and directing the information to be assimilated in the higher-end process of intelligence research.

In reviewing both processes described above, metaknowledge is critical in developing a synergic project for the intelligence community of practice and security beneficiaries.

What is metaknowledge? Metaknowledge is a concept that has only recently started being used to understand how knowledge is accessed and processed in social networks, or communities of practice, where such morphology has been already implemented. There is a relatively low yield of

articles that treat metaknowledge from other perspective than that of computer science, which is the source of the concept.

Referring to patterns of scientific content, Evans & Foster (2011) define metaknowledge as knowledge about knowledge, a scientific process which aims to uncover patterns and regularities, infer beliefs and create tools to research. Following their operational definition, metaknowledge is a dynamic instrument meant to "reshape science", based on a networked morphology. Chen (1993) views metaknowledge as a feature of knowledge-based systems and has relation with the way in which knowledge is accessed and applied during the search of a solution. Adding to the above definition, Paquette (1999) considers metaknowledge an instrument to autonomous learning, taking as reference information technology learning systems, where a knowledge model is assimilated with a learning events network.

According to Chen (1993, p. 81), metaknowledge is important because it supports: 1. knowledge acquisition – the knowledge needed to maintain the influx of knowledge, and 2. inference control – controlling the application of rules by organizing and prioritizing. Both morphologies are consistent with the needs of the intelligence process dynamics.

Therefore, metaknowledge is understood in this study as an ensemble of models providing the user with an enhanced system of knowledge assessment, together with strategies to applying that knowledge to specific domains and purposes, integrated in a networked learning morphology.

Introducing the concept of metaknowledge in the usage of the intelligence domain is a natural step in understanding and solving the communication and adaptation requirements scholars and practitioners in intelligence have, to be able to exchange critical knowledge at low risk.

China and the Chinese Intelligence system as topics for Intelligence research

Before engaging in evaluating the state of research regarding China's intelligence system, there are some metatheoretical considerations to be made about China as an overall subject for the intelligence community.

Firstly, there is the issue of defining China as a subject of research. Due to factors pertaining to the political-administrative migration policies and technological implementation policies, China is to be understood for intelligence analysis purposes as concept, more than a national state actor. Secondly, there is also the reference to Chinese ethical norms, influencing political action and outcomes, a subject which is deeply misunderstood and remains a subject of inquiry for intelligence research. Lastly, there is the issue

of theoretical approach to integrating China in a manageable perspective for policymakers. In a political philosophy representation, the Chinese politico-administrative-social nature is yet to be addressed in theoretical frameworks, and to produce new theoretical effects and analytic methodologies.

It's worth mentioning here the active debate between the adepts of China as part of the mainstream theoretical framework and those which favour the representation of China in a contextual approach. Both perspectives would produce analytical effects for strategic intelligence. Based on the above-mentioned prerequisites, I argue that the Chinese intelligence system is the product of the Chinese socio-political nature, cultural norms and a vast assortment of policy experimentation.

Studying the effects of metaknowledge for the development and understanding of the Chinese intelligence system, there are two vantage points to be considered.

a. Metaknowledge usage in the Kentian intelligence system

From the Kentian intelligence community perspective, the metaknowledge production is related to accessing information from a historically opaque political system. In respects to its organization, the Chinese intelligence system has an organizational structure similar to that of the intelligence services in United States, or the UK, and intelligence statecraft is similarly defined.

However, China combines simultaneously in governance normative and positivist perspectives on politics and social development. Until now, there is no theory that can be applied to explain the Chinese political system, and this is mostly due to the lack of a control variable (or a similar example to compare it with). Western researchers used information analysis to understand the Chinese system, which offered an extensively branched research field, but no integrated theory. From this point of view, metaknowledge research could be used to fill this gap.

b. Metaknowledge usage in the Chinese intelligence system

The Chinese political elite became extensively interested in developing this field, especially by innovating in artificial intelligence. There is funding from the central government meant to develop the metaknowledge concept as an inference method to big data. This effort is also supported by its adaptive authoritarianism features, which uses local experimentation in order to combat risks to political instability. Hence, China uses metaknowledge in its philosophical acceptance, as well as part of the information science revolution, supported by high financing from the central government.

For intelligence theorists and practitioners, referring to China became a positivist vision about a normative political system, which creates analytical problems. Therefore, creating a theory based on metaknowledge research in order to explain it represents the most feasible option.

The meaning of intelligence as accepted in Chinese governmental sphere remains similar to the definition of strategic intelligence, as it was proposed by Sherman Kent (1949, p. VII), as "knowledge vital for national survival". Kent's project for a national community of intelligence would have been based on specialized bureaus housed within the departments of the executive branch, following the decentralization logic. However, the project was rejected by the Congress. (Greenberg, 2007, p. 171).

In order to use metaknowledge for intelligence purposes, it is necessary to understand the research sources and methods that should stay at the basis of the Chinese intelligence statecraft, by bridging the knowledge about areas of study with the methods and its afferent metaknowledge.

In a recent article, Peter Gill & Mark Phythian (2016) identified four main areas when analysing the development of intelligence studies, as follows: the research/historical, definitional/methodological, organizational/functional, and governance/policy perspective. I am using the same categories, to outline the fact that the Chinese intelligence is a multidimensional system, source:

- *The research/historical approach*

No matter the period of time, western research literature has been one step behind concerning China's security system. At the end of the Cold War, the access to reliable sources informing about the intelligence services, their modus operandi, and the historical path, it was relatively scarce. This was also due to the ideological heterodoxy of the Chinese communist party. But maybe the worst aspect was the deeply flawed methodology used to study them, counting mostly on journalist reporting, more than on scholarly research. In the 80', along with the elite change, public intelligence history publications started to appear, one of the reasons being that the Ministry of State Security gains diplomatic reputation abroad (Chambers, 2012), making the relative access to information a strategic vision promoted by the CCP. This situation is reported today, when there is almost no integrated knowledge about the Chinese contemporary intelligence capabilities, especially regarding collection against foreign targets (Inkster, 2013).

- *The definitional/methodological approach*

One approach to Chinese intelligence is the "mosaic" or "grains of sand" strategy, which is explained by four basic assumptions. According to Mattis (2012, p.48-40), Chinese intelligence collection is based on the work of ethnic Chinese, more likely to be amateur collectors rather than professional

intelligence officers. The Chinese intelligence tends to use unclassified information. Even though Chinese intelligence resembles the western intelligence statecraft where intelligence is defined as a specialized form of knowledge with the purpose of reducing uncertainty during decision making, in practical terms, the Chinese intelligence is more connected with the social environment in which it operates.

- *The organizational/functional approach*

Peter Mattis explains that the analysis of intelligence institutions is another way to know more about how the Chinese government uses information to formulate policies, to guide diplomats and security officials, and to implement policies. Contrary to the western intelligence, Chinese civilian intelligence and security agencies have the authority to operate outside the Chinese borders, since there is an irrelevant distinction between strategic intelligence and internal security. This is due the fact that the purpose of state security policy is to keep the integrity and power position of the Communist Party of China (Mattis, 2012, p. 47).

Chinese Intelligence and Security Services[2]	
Civilian	**Military**
Ministry of State Security (MSS) Counterespionage and Counterintelligence; Foreign Intelligence; Domestic Intelligence	*Second Department of the People's Liberation Army* (PLA) *General Staff Department* (2PLA) Foreign Intelligence; Defence Attaché System; Imagery Intelligence; Tactical Reconnaissance
Ministry of Public Security (MPS) National Police; Domestic Intelligence;	*Third Department of the PLA General Staff Department* (3PLA) Signals Intelligence

- *The governance/policy approach*

The governance approach to policing is represented with the term "adaptive authoritarianism" (Perry and Heilmann, 2011). The meaning of the term implies that the political regime is able to resist to systemic disturbances, and furthermore, to adapt and further resilience (Perry and Heilmann, 2011,

[2] Other major intelligence and security departments not specifically discussed in this essay include the Fourth Department of the PLA General Staff Department (4PLA); the Liaison Office of the PLA General Political Department; the intelligence departments of the PLA Navy, PLA Air Force, and Second Artillery; and the State Secrecy Bureau.

p.11). China's local experimentation represents an instance of adaptability to local disturbances.

Experimenting with metaknowledge

According to Lewis Husain (2017), there is a specific Chinese model of development that supposes experimental policy-making and policy innovation to reform complex systems, systems that require metaknowledge to make use of adapted policies (reported previously by Daniel A. Bell, 2006). He applies the Chinese experimentation paradigm to the reform of the Chinese health system of the '90s. (2017, p. 5) and proposes four typologies of experimental policies which can be applied in China for developing complex systems.

The proposed typology shows that in the case of previously partially successful counties, the central government tended to allow a more decentralized framework in implementing pilot policies.

Typology of China's experimental policy processes[3]	
Indicative type	**Salient features**
TYPE I: MANAGED PILOTING/POLICY TRIALING • Extended oversight, central government expertise	- Direct experimentation, allowing trialling of targeted interventions in which pilots are relatively closely managed with the intention of trialling specific approaches to defined policy problem; local governments have a relatively low degree of discretion - Technical support to implementing units is often provided by research institutes, academics, and/or international agencies; local governments retain discretion in concrete management approaches adopted and in timing, etc., in an attempt to find approaches with contextual fit - Pilots may be in advance of the national (or provincial) policy agenda, and have an agenda setting function, or

[3]Adapted from Husain, 2017, originally entitled "Indicative typology of China's experimental health policy processes", in reference to health reform from the '90s onwards.

	may fall within existing policy frameworks and form part of ongoing reforms and may provide lessons of supra-local or systemic significance - Screening and learning: scale up of practices deemed useful may or may not take place; may be directed by higher levels of government (frequently through one size doesn't fit all scale up) or may be relatively organic
TYPE II: EXPERIMENTAL POLICY FRAMEWORKS; LOCALGOVERNMENT PURPOSIVE REFORMS • Implementation choices made available to the local governments	- Framework policy is set by central or provincial government, giving local governments or other implementing units limited discretion between relatively defined implementation choices; leads to multiple practices - Implementing counties often have little expert support or technical assistance, though better-resourced jurisdictions may have support from national or sub-national research institutions, or occasionally external TA through international programmes; space for pragmatic problem solving and emergence of 'appropriate' approaches with contextual fit - Local government reforms fall within the 'implementation' phase of the policy cycle; may provide lessons of supra-local or systemic significance - Screening and learning: as above
TYPE III: OPEN POLICY FRAMEWORKS; LOCAL GOVERNMENTADAPTIVE INNOVATION AND LEARNING BY DOING • Relative autonomy to decide own reforms	- 'Open' policy frameworks are used by central government, allowing space for broad local discretion in implementation and learning by doing and emergence of multiple practices - Often little expert support – as above; space for pragmatic problem solving and emergence of 'appropriate' approaches with contextual fit

	- Local government innovation falls within the 'implementation' phase of the policy cycle; may provide lessons of supra-local or systemic significance - Screening and learning: as above
TYPE IV: DECENTRALISED IMPLEMENTATION; RANGE OFPOLICY PRACTICES • Contextual policy practices	- Decentralized policy making in the absence of national standardization can produce a range of policy practices - Often little expert support – as above; space for pragmatic problem solving and emergence of 'appropriate' approaches with contextual fit - May fall in multiple phases of policy cycle; may provide lessons of supra-local or systemic significance - Screening and learning: as above

From a theoretical perspective, intelligence exploits metaknowledge to obtain efficient models and solutions. Metaknowledge stands for knowledge to be exploited from past learning tasks, which may both mean past learning tasks on the same data or using data of another problem domain (Lemke & Budka, 2015). The clue obtained from the health system reform case reported by Lewis Husain (2017) shows that policing in China tends to resort to local experimentation and exploits metaknowledge retrieved from this type of policing.

Current accounts about security policy in China report about adapted local policies, which take the form reflected by the above-mentioned experimentation case regarding the health system. With the help of a largely improved communication system, – which established the „information society" in China (Mattis, 2012, p. 48). Based on a heavily regulated social system, metaknowledge is no longer a challenge for the Chinese government.

Moreover, the combination between vertical and horizontal lines of authority, as well as the „open policy framework" assures that the system remains flexible enough to permit shifts in experimentation policies.

In order to further exemplify previous ideas, I am referring to the Golden Shield Project and the Social Credit System, two governmental policies implemented after successful local experimentation.

The Golden Shield Project: The Golden Shield was one of twelve projects started in the 80s, with the main strategic goal of creating an e-government infrastructure, and the declared goal of improving communication between the Chinese people and their government, and increase efficiency in policy implementation (Guo, 2006). Following several years of experimentation at local level, this intelligence policy was eventually implemented nation-wide. In 2008, the Ministry of Public Security inaugurated the „public security informatization" policy, which was meant to closely integrate collected information into the intelligence and public security management components (Mattis, 2012:50). The goal of Information and Communication Technologies (ICT) development in China, "to deepen administration system reform, further transform government functions, improve management style, promote e-government, enhance administrative efficiency, reduce administrative costs, and form a standardized, harmonious, fair, transparent, clean, and effective administrative system." is based on the directive of the former secretary general of the Communist Party of China, Jiang Zemin (Guo, 2006:3).

The Social Credit System

Briefly put, China's Social Credit System (社会信用体系 *shehui xinyong tixi*) is a real-time social reputation rating system. Individual reputation is measured by the level of compliance of a person towards specific governmental rules, norms, and policies, and is enforced by a broad range of rewards and punishment methods (Ohlberg, et al., 2017, p. 4). The first steps of the project have been made in 2003, with experiments at provincial level. In 2016, 11 pilot cities have been chosen to test the implementation of the system, followed by another 32 cities, later that same year (Ohlberg, et al., 2017, p. 9). Legislation is currently underway for the lasts steps in nation-wide implementation and popularization media campaigns have already been released at national level. The Social Credit System is based on the ICT framework developed according to the Golden Shield project principles.

The above-described projects have fundamentally changed the principles of governance in China and there are yet to set the foundation for further reforms. Governance moved into cyberspace and the metaknowledge resources and possibilities to be used by the Chinese intelligence became overwhelming.

Concluding remarks

The purpose of this article was to outline certain theoretical concerns related to the research about the Chinese intelligence system, the understanding of China's political and administrative specificity and to draw attention on the need to focus on metaknowledge production as explanatory and defining for future governance and intelligence policies in China. I argued that intelligence policies in China are subject to local experimentation and that metaknowledge is the key to predicting governance actions. Assessing the Chinese intelligence, – for scholars and practitioners alike – should be predetermined by a meta-theoretical strategy, used as basis for a new theory that integrates China as concept and as strategic node in dynamic networking.

References:

1. Chambers, David Ian, (2012), "The Past and Present State of Chinese Intelligence Historiography", *Studies in Intelligence*, Vol. 56, No. 3, pp. 31-46.

2. Chen, Z., (1993), "On Continuous AI and Meta-knowledge", *Kybernetes*, Vol. 22, No. 4, pp. 78-84.

3. Evans, James A., Foster, Jacob G., (2011), "Metaknowledge", *Science*, Vol. 331, pp. 721-725.

4. Gill, Peter, and Phythian, Mark, (2016), "What is Intelligence Studies?", in *The International Journal of Intelligence, Security, and Public Affairs*, Vol. 18, No. 1, pp. 5-19.

5. Husain, Lewis, (2017), "Policy experimentation and innovation as a response to complexity in China's management of health problems", in *Globalization and Health*, 13, p. 54.

6. Johnson, Loch K., (2007), *Strategic Intelligence*, Vol. 1-5, Praeger Security International, Westport, Connecticut, London.

7. Kent, Sherman, (1949), *Strategic Intelligence for American World Policy*, Princeton: Princeton University Press.

8. Lemke, Christiane, Budka, Marcin, Gabrys, Bogdan, (2013), "Metalearning: a survey of trends and technologies", Artificial Intelligence Review, Vol. 44, No. 1, pp. 117-130.

9. Liang, Guo, (2006), Under the "Golden Shine": China's Efforts to bridge Government and Citizens, Centre for Social Development, Chinese Academy of Social Sciences, January 28, pp. 1-20.

10. Mattis, Peter, (2012), "The Analytic Challenge of Understanding Chinese Intelligence Services", in *Studies in Intelligence*, Vol. 56, No. 3, pp. 47-57.

11. Mezey, G., (2004), "The cybernetic paradigm". Retrieved from http://www. armyacademy. ro/reviste/2 2004/r16. pdf.

12. Ohlberg, Mareike, Ahmed, Shazeda, Lang, Bertram, (2017), "Central Planning, Local Experiments: The Complex Implementation of China's Social Credit System", Mercator Institute for China Studies, December 12, pp. 1-15.

13. Paquette, Gilbert, (1999), "Meta-knowledge Representation for Learning Scenarios Engineering", Télé-université, LICEF Research Centre, Conference Paper, Montreal, accessible on http://www.licef.teluq.uquebec.ca.

14. Perry, Elizabeth J. and Heilmann, Sebastian, (2011), *Embracing Uncertainty: Guerrilla Policy Style and Adaptive Governance in China*. In *Mao's Invisible Hand: The Political Foundations of Adaptive Governance in China*, eds. Elizabeth J. Perry and Sebastian Heilmann, pp. 1-29. Cambridge, MA: Harvard University Press.

15. Thompson, Paul, Nawaz, Raheel, McNaught, John, Ananiadou, Sophia, (2017), "Enriching news events with meta-knowledge information", Vol.51, No. 2, pp. 409-438.

16. Treverton, Gregory F., Jones, Seth G., Boraz, Steven, and Lipscy, Philip, (2006), *Toward a Theory of Intelligence: Workshop Report,* Santa Monica, RAND.

AN INTELLIGENCE-BASED APPROACH TO COUNTERING SOCIAL MEDIA INFLUENCE OPERATIONS

Matteo E. BONFANTI*

Abstract

The paper describes an intelligence-based approach to identify, understand and counter influence operations and campaigns that are sponsored, directed, or conducted by State or non-state actors on/through social media platforms. It examines the extent to which the collection and analysis of social media data and further contextual information can provide actionable insight into influence-aimed activities perpetrated by both State and non-state actors. It also discusses how to employ such insight for tailoring effective counter-measures at the operational, tactical and strategic levels. The paper starts by conceptually framing social media platforms and services as tools for exercising influence – or cyber-influence/persuasion – over a target. For this purpose, it examines the notions of "influence operations" and/or "campaigns", presents their featuring elements, and shortly discusses if, how and to what extent they have changed or are changing due to the emergence of the cyber-space and new technological platforms. The study benefits from the review of the recently available literature dedicated to the employment of social media for influence purposes as well as the examination of few selected and documented case studies. Then the paper examines the crafting of intelligence on influence operations form social media data and metadata, in particular on actors engaging in these operations, their employed capabilities, modus operandi, intended goals as well as the operational constraints they face. It outlines the collection and analytical techniques serving the purpose of producing social media intelligence, presents their general advantages and limits, and highlights the challenge of enriching the knowledge on influence operations with further contextual information and intelligence. The paper concludes by proposing recommendations on how to implement the intelligence-based approach to countering influence operations or campaigns over social media in an effective manner. These include the acquisition of the necessary capabilities (human, technological, and organisational) to monitor and analyse social media information. They also include the definition of a framework to better integrate intelligence from social media in to a consistent all-source intelligence system.

* Senior Researcher dr., ETH Centre for Security Studies, Zurich, Switzerland, matteo.bonfanti@sipo.gess.ethz.ch

Keywords: *Influence, Social media, Cyber-influence, Intelligence, Counter-Intelligence*.

Introduction

On May 27-28th 2018 and in the following days, the Italian President of the Republic was the object of an intensive Twitter messaging campaign asking for his resignation. (Sarzanini, August 5, 2018; Giuffrida, Kirchgaessner and Henley, May 27, 2018)[1] The campaign was triggered by the President's refusal to appoint the recently-formed parliamentary coalition' proposed minister of finances. It endorsed different statements aimed at discrediting the President, accusing him of "high treason", and sustaining his impeachment. Echoed by other new and traditional media, the campaign put a certain political pressure to the holder of Italy's highest institutional post.[2] In the short-term, it polarised part of the Italian public opinion around supporters and opponents of the President, exacerbated some of the prevailing divides between political coalitions, and reinforced existing frictions among social groups and individuals (Riformato, May 27, 2018).[3]

The content, reach and timing of the campaign, its observable dynamics and likely intents, as well as the fact it addressed the President Office prompted an investigation by the Italian authorities. The investigation – which is presently on-going – aims at ascertaining whether the *twits* and further on-line messaging "storm" pursued subversive or other criminal goals.[4] At the same time, it points at identifying the entities who initiated, fuelled, promoted, probably coordinated the spreading of messages, and are

---

[1] #mattarelladimettiti ('#mattarellaresign'), #mattarellavergognati ('#shameonyoumattarella'), #mattarellanonèilmiopresidente ('#mattarellaisnotmypresident'), #mattarellaimpeachement, were the most popular hashtags used in the Twitter messaging campaign.

[2] Thematic pages, posts and videos against the President of the Italian Republic were created and disseminated also through Facebook and Youtube. See for example, https://it-it.facebook.com/pages/category/Community/Sergio-Mattarella-Non-%C3%A8-il-Mio-Presidente-585198994957256/.

[3] #iostoconmattarella is one of the most popular hashtags adopted by Twitter users to express their support to the President.

[4] The investigation is directed by the Anti-Terrorism Prosecutor Office in Rome who can rely on the support of the Italian Postal Police. It is based on art. 277 "Attack on the freedom of the President of the Republic" and art. 278 "Offense to the honor and prestige of the Head of State" of the Italian Criminal Code. Given the national security related implications of the case, the Director of the Italian Department of Information Security was asked to report on it to the Parliamentary Committee for the Intelligence and Security Services.

responsible for that.[5] In this regard, preliminary indicators and limited evidence drew non-domestic entities in to play. They suggested the possible involvement of foreign States or state-sponsored actors who have the capabilities to employ social media platforms and services systematically for achieving pre-defined goals.[6] Actors have already engaged in similar initiatives but in other geographical, political and social contexts, and who might have interests in interfering with Italy's domestic institutional processes. In particular, actors who had resorted to social media content to trigger public pressure on policy-makers abroad and affect their decisions-making processes, undermine their leadership, obtain political paralysis, erode civil society's trust in local institutions, or amplify social divisions. Speculations about the involvement of the above foreign entities were triggered also by some observable patterns of the Twitter campaign against the Italian President, *i.e.* the employed tactical scheme and modus operandi (obviously not the content!) as well as its apparent short-terms results (polarisation and erosion of public trust).

Initially, suspects addressed a Russia-related agency, which had already been reported for using Twitter, Facebook, VKontakte or other social and on-line media in the above-described fashion (Fubini, August 3, 2018; Roeder, 2018).[7] However, this agency is not the only player in the arena. Other Countries run or sponsor similar activities (FireEye, August 2018); and even private organisations could engage in to them, both on the smaller and larger scale.[8] Indeed, results from further technical analysis depict a more articulated

---

[5] See art. 494 "Impersonation" of the Italian Criminal Code. *Cf*. also "Ipotesi illecita: sostituzione di persona (art.494 c.p.)" at https://www.commissariatodips.it/approfondimenti/social-network/approfondimenti-normativi.html.

[6] There is no agreed definition of social media in the literature and among practitioners. In plain language, the expression refers to the Internet-based technologies and practices that allow users to generate and share information in different formats, and to establish relations among them.

[7] As reported by the media, at least twenty Twitter profiles proactively involved in the campaign against Italian President were employed by the Internet Research Agency (IRA) of Saint Petersburg in other propaganda campaigns in favour of populist parties, sovereigntists, and anti-Europeans. These findings emerged from the parallel analysis of a vast repository of IRA-attributed tweets collected by researchers from the Clemson University and provided to the US prosecutor Robert Mueller as part of the investigation of the Russian influence on the 2016 US Presidential elections. The repository includes tweets in Italian, which originated from accounts that were fuelling discussions against government representatives.

[8] See the strategic communication operations run by the private company Cambridge Analytica during the electoral processes in targeted countries. See BBC News, "Cambridge Analytica: The data firm's global influence", accessed 24 September 2018 at https://www.bbc.com/news/world-43476762.

scenario. As far as Twitter is concerned, the user's profile who started the messaging campaign against the President was probably registered in Italy — through the Milan's data hub — but shielded in such a way as to make it seem to originate abroad. Other accounts (at least 150) were suddenly created through servers located in Estonia or Israel. Then, in a very short-time period, about 400 new Twitter profiles generated an anomalous spike in the number of messages against the President. As reported by the media, the campaign originated from a single source, most likely an "Italy-based organisation specialized in this type of activities" (Sarzanini, August 5, 2018).[9] It has still to be clarified whether the organisation acted for its own purposes or as a proxy for other domestic or foreign entities. It goes without saying this is a crucial issue given the implications it may generate from legal and political point of views as well as in terms of the responses that may follow. If ascertained, the involvement of foreign entities will make national security considerations prevailing over those related to the maintenance of the public order and rule of law. In principle, it may prompt diplomatic, economic, military and informational counter actions further to those enacted at the law enforcement and judiciary level.

Pending the above salient issue as well as the results from additional forensic investigation, it is somewhat evident the Twitter campaign promoters' intent to mobilise a segment of the Italian social media users' community and, more broadly, the wider national public opinion. By adopting a certain degree of deception and by exploiting the vulnerabilities of the system of opinion formation within social media, they tried to orient and condition the targeted users' decision-making processes, modify or reinforce their attitudes, alter their perceptions, shape their judgments through persuasion, and induce a specific behaviour (Pamment, Nothhaft, Agardh-Twetman, and Fjällhed, 2018, pp. 20-21). They acted within the informational environment, especially in its cognitive or semantic dimension, by employing information as a tool for persuasion and influence (Floridi, 2010, p. 3; Durante, 2017, pp 21-37).[10] They orchestrated the dissemination of messages fostering antagonism and confrontation on a specific issue; supported and amplified a non-constructive narrative which can be considered disproportionally

[9] The most probable hypothesis is that the organisation used Tor, a software permitting anonymous online communication by means of encryption, to prevent its identification.

[10] The informational environment is a complex domain in which agents operate through information and interact on the informative level. Also called "infosphere", it is "constituted by all informational entities, their properties, interactions, processes and mutual relations. It is an environment comparable to, but different from cyberspace (which is only one of its sub-regions), since it also includes off-line and analogue spaces of information".

disruptive of social cohesion. At the very first sight, the above suggests they engaged in activities/operations that could be technically considered "inform and influence"; or – given both the domain where these activities/operations occurred and the tools employed to carry them out, i.e. the Internet and social media –"cyber-/social media influence" (Brangetto and Veenendaal, 2016; Szafranski, 1997, pp 395-416; Arquilla and Ronfeldt, 1997, pp. 1-20).[11] These types of activities are different from genuine journalistic, public affairs, civil-society, marketing, and public relations initiatives or lobbying. They are also different from open (on-line or off-line) political campaign and debate, or public diplomacy. Their general lack of transparency coupled with their potential or actual harmful impact on individuals and society put their legitimacy in to question.

How can governments safeguard their interests and tangible or intangible assets from illegitimate cyber- and social media influence operations? What kind of actions should they take to prepare, prevent, respond and recover from these activities? What capabilities do they need? The existing literature on information influence activities provides useful answers to these framework and other more specific questions. The same does the literature covering specifically influence operations through the Internet and social media. In general, they suggest the adoption of multi-discipline (normative, educational, technological, law enforcement), multi-layer (local, national and international), multi-sector (public and private) and multi-stakeholders (governmental institutions and agencies, social media platforms and services providers, users and civil society) coordinated counter-measures. To be effective, these measures should be premised upon a genuine understanding of cyber-social media influence operations, in particular of the actors engaging in the operations (domestic or foreign), the activities they carry out, the strategies, doctrines and principles to which they are informed, the organisational aspects involved and resources needed, the tools, tactics and techniques they employ, their intent and observable results. From a

[11] There are several definitions and connotations of "influence operations". In general, "influence" refers to a broad range of activities including the use of corruption, coercive economic means, public pressure exercised by political parties, think tanks, academic institutions, and the exploitation of ethnic, linguistic, regional, religious and social tensions. Expressions alike "Information Warfare" (IW), "Psychological Operations" (PsyOps), "Strategic Communications" (STRATCOM), "Computer Network Operations" (CNO), and "Military Deception" (MILDEC) refer to operation in the informational domain that are more or less covered by the umbrella term "Information Operation". In addition to the cited labels, terms as diverse as "neocortical warfare" and "net war" have all been used to describe attempts by one or all sides in a conflict or dispute to either change their opponent's position, weaken their resolve or undermine a prevailing narrative.

prevention point of view, such an understanding would support the detection of imminent and on-going cyber- and social media influence operations.

At the tactical and operational level, detection can specifically profit from the collection and analysis of social media data and further contextual information. This intelligence can provide actionable insight into influence-aimed activities perpetrated by both State and non-state actors. The present paper discusses the crafting of such intelligence. It starts by conceptually framing social media platforms and services as tools for exercising cyber-influence over a target. For this purpose, it examines the notions of "influence operations" and/or "campaigns", presents their featuring elements, and shortly discusses if, how and to what extent they have changed or are changing due to the emergence of the cyber-space and new technological platforms. The study benefits from the review of the recently available literature dedicated to the employment of social media for influence purposes as well as the examination of few selected and documented case studies. Then, the paper examines the crafting of intelligence on influence operations form social media data and metadata, in particular on actors engaging in these operations, their employed capabilities, modus operandi, intended goals as well as the operational constraints they face. It outlines the collection and analytical techniques serving the purpose of producing social media intelligence, sketch their general advantages and limits, and highlights the challenge of enriching the knowledge on influence operations with further contextual information and intelligence. The paper concludes by proposing broad recommendations on how to implement the intelligence-based approach to countering influence operations or campaigns over social media in an effective manner. These include the acquisition of the necessary capabilities (human, technological, and organisational) to monitor and analyse social media information. They also include the definition of a framework to better integrate intelligence from social media in to a consistent all-source intelligence system.

Cyber-influence through social media: is there anything New under the sun?

National governments or sub-national entities have resorted to inform and influence operations or campaigns several times in history – in peacetime, within a rivalry or situation of tension, and during open conflict/warfare

(Costello, 2018).[12] The objectives, targets and techniques involved in these operations are not new.[13] Nor are the strategies and stratagems typically employed to run them (Pamment, Nothhaft, Agardh-Twetman, and Fjällhed, 2018). Especially when carried out by or on behalf of foreign entities, influence operations become relevant from a national security perspective because they interfere with the established institutional processes and functions of a State, and invade its sovereign space. Targets of influence may vary from a region's civilian population, selected decision-makers, military personnel, to governments or State institutions. In other words, influence operations can feature in "social" information activities as they target the society as a whole or social groups, in particular those groups' ideas, opinions, motivations and beliefs. They can also entail "individual-oriented" activities as they address selected individuals with a specific psychographic profile. In both cases, they tactically aim at affecting psychological processes, shaping motivations or ideas, conditioning behaviour and choices (Palmertz, 2017).

Whereas the fundamental goals and objectives of inform and influence operations or campaigns have not significantly changed over time, the tools and techniques to achieve them have. They have evolved alongside socio-economic-cultural changes, also because of the development and use of new information and communications technologies, the Internet included. These technologies have progressively transformed the information environment in its constituent elements and inherent dynamics (Pamment, Nothhaft, Agardh-Twetman, and Fjällhed, 2018, p. 20).[14] They have contributed to generate an additional dimension or space, the so-called cyberspace, within which a wide range of agents (not only States) can use information for several purposes,

[12] For example, during the First World War the Allies engaged in propaganda activities by dropping leaflets over German soldiers, calling on them to surrender. Conflicting parties ran similar actions during the Second World War, the Cold War, the two wars in Iraq, and, more recently, in conflict areas like Libya and Syria. Resort to information operations in peacetime or within hybrid-conflicts is also very common as, for example, the alleged use of media and information in Turkey shows.

[13] The difference between "operation" and "campaign" concerns the scope, reach, objects and time-frame of the influence activities and actions they consist of as well as the level of coordination among them. Generally, while an operation encompasses a smaller and more specific objective to be achieved with tactical actions run within a mid/short time-frame, a campaign entails a coordinated set of operations aimed at achieving strategic objectives on the longer run.

[14] As explained by James Pamment the impact of technological innovations on the information environment is coupled by the commercial reconfiguration of large parts of the media system (especially in Western countries). Such reconfiguration has prioritised commercial imperatives over the reliabilities of the information sources and integrity of the information.

including influence-related ones.[15] Cyber-influence (or persuasion) is the recently coined terminology to refer to inform and influence operations that are run in the cyberspace, leverage this space's distributed vulnerabilities, and rely on cyber-related tools and techniques to affect an audience's choices, ideas, opinions, emotions or motivations.[16]

Compared to "traditional" inform and influence activities, cyber-influence employs context-specific tools and techniques to achieve its goals. It takes advantages of how social media platforms and services are designed and work. It profits from how information is generated, distributed and consumed by social media users, as well as from the way they interact and establish relationships among themselves. To a certain extent, social media platforms make cyber-influence easier, cheaper and faster to carry out.[17]

They present some intrinsic features that make them both the preferred terrain/environment and tool/capability for engaging in cyber-influence. "They enable precision-targeted messaging and advertisement based on psychographic targeting at an unprecedented dimension of contemporary information influence activities" (Pamment, Nothhaft, Agardh-Twetman, and Fjällhed, 2018, pp. 25, 26, and 28). At the same time, they allow to reach out a wide and geographically distributed audience. They combine text, photos, videos and audios clips (*e.g.* memes) that are amenable to manipulation and misappropriation through simple techniques.[18] They make mechanisms of information scrutiny and source review more complex. By allowing deception and supporting automation, these platforms hinder accountability processes and makes attribution difficult (Pamment, Nothhaft, Agardh-Twetman, and Fjällhed, 2018, pp. 30-31).[19] Finally, actors proactively

[15] With the advent of the cyberspace, the control and release of information is no longer the purview of few established actors. Every organisations and even ordinary individuals can reach mass audiences through online platforms.

[16] Cyber-influence or persuasion makes use of information and communications technology and networked systems. Unlike "technical" information operations such as computer network operations (CNO) – in their variant of Computer Network Defence (CND), Computer Network Exploitation (CNE), and Computer Network Attacks (CNA) – Cyber-influence does not target an enemy's or opponent's technical assets such as data servers or network nodes. It targets individuals or groups' minds. It goes without saying that cyber influence can be used in combination with technical information operations.

[17] At a very basic level, an actor only needs an internet-enabled device, freely available account-based applications, an elementary knowledge of how to use social media, and an internet connection.

[18] Manipulation can also be quite sophisticated as "deep fake" videos shows.

[19] "Today networked individuals are exposed to fragmented messages, many, like memes, without ascertainable factual content, many without an identifiable source, many only in the flow because they are shared by friends or promoted by algorithms".

engaging in to social media influence can count on the – more or less unconscious – support from users behaving as "useful idiots". These are users who act and process information uncritically, and that amplify the magnitude of the operation. Their active presence and participation in disseminating information makes the detection of the operations even more difficult.

However, the potential of cyber-influence, in general, and social media influence, in particular, should not be overestimated. First, social media penetration is variable across geographical regions and segments of the population. Second, research shows that people rarely rely on the Internet and social media as their unique or primary source of information. Television and other offline media outlets are still the dominant platforms for news. Furthermore, information and news are often sourced from family members, friends, and community leaders. The above also explains why influence operations or campaigns generally entail the synchronised use of different sources of information and involve actors like NGOs, think tanks, individual agents (*e.g*. celebrities, religious leaders) that operate "off-line" too.

A closer look in to social media influence operations

Social media influence operations and campaigns can be quite complex, rely on extensive planning and preparatory activities, and draw upon different techniques and stratagems. Each operation or campaign has its own specific features. Nevertheless, most of them adopt similar tactical schemes and modus operandi.

Among other things, planning for social media influence operations involves intelligence-gathering activities.[20] It requires identifying exploitable vulnerabilities and targets. Identification may rely on different methodological concepts and approaches as well as on automated or semi-automated techniques and technologies like "crawlers", "spiders" or "monitoring bots".[21] With regard to vulnerabilities, they may concern the platforms' design and functions, their communities of users, and the social-cultural and political contexts to which users belong. Examples of these "technical-technological", "human-related" and "societal" vulnerabilities are: exploits in the platform' provided privacy and security setting or other technical features (API

[20] Intelligence gathering is often conducted prior or in concert with influence operations because it helps in identifying the best courses of action.

[21] "Bots" is a shorter term for robot. It is an automated program which performs repetitive actions along a set of algorithms. It can collect data on the platforms and their users and make these data available for analysis. Simon Hegelich, "Invasion of the social bots" (Berlin: Konrad Adenauer Stiftung, 2016).

applications or widgets); selected users' personal information to be leveraged for malicious purposes (*e.g.* blackmailing or for compromising accounts); and existing socio-economic frictions and political divides.[22] Scouting vulnerabilities is coupled with targets reconnaissance activities. Targets can range from wider audiences, specific groups, to individuals (*e.g.* influencers). They can be identified via psychographic or socio-demographic profiling carried out through more or less advanced technological applications and techniques.[23] The case of Cambridge Analytica is an example of using psychographic targeting to understand users' preferences (Gibney, 2018). Similar techniques were apparently used also with regard to the US presidential election in 2016. According to the FBI, the Russia-related Internet Research Agency (IRA) initiated its influence operation in 2014 by conducting a comprehensive target audience reconnaissance and psychographic mapping of US social media sites dedicated to politics and other social issues.[24] IRA's goal was to determine metrics such as reach, audience engagement, frequency of posts, and nature of content. This baseline knowledge provided a point of departure for the operational design of social media influence activities (Pamment, Nothhaft, Agardh-Twetman, and Fjällhed, 2018, pp. 79-81).

Coming to the techniques that are suitable for engaging in to social media influence, they are different. They include socio-cognitive and psychographic hacking via dark advertisement, social hacking, band wagering, digital disinformation and fakes, exploitation via bots, botnets and sock-puppets, trolling and flaming (Pamment, Nothhaft, Agardh-Twetman, and Fjällhed, 2018, pp. 31-79). Most of these techniques are used in combination; they result in stratagems like polarisation, enraging, flooding and laundering

---

[22] In some cases, scanning for human-related vulnerabilities is based on ad hoc activities like the creation of honeypots to solicit information via malicious links. Trend Micro "Hackers Exploit Instagram API Flaw to Steal Information from Verified Users", accessed 24 September 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hackers-exploit-instagram-api-flaw-to-steal-information-from-verified-users; Rob Hornbuckle, "Social Media Vulnerabilities and Considerations for the Corporate Environment", 2016, accessed 24 September 2018 at http://www.infosecwriters.com/ Papers/ RHornbuckle_Social_Media.pdf; Candid Wüest, "The Risks of Social Networking", 2010, accessed 24 September 2018 at https://www.symantec.com/content/en/us/enterprise/media/ security_response/whitepapers/the_risks_of_social_networking.pdf.

[23] While the former concerns the segmentation of users depending on their personality traits, values, preferences and attitudes, or other features, sociodemographic profiling discriminate users according to their age, gender, education, ethnicity. See https://www.cbinsights.com/ research/what-is-psychographics/.

[24] United States of America V. Internet Research Agency LLC, Case 1:18-cr-00032-DLF, accessed 24 September 2018 at https://www.justice.gov/file/1035477/download. See "Intelligence-Gathering to Inform U.S. Operations", par. 29; see also par 37.

(Pamment, Nothhaft, Agardh-Twetman, and Fjällhed, 2018, p. 70).[25] For example, polarisation entails supporting opposing views on one or more issues. It aims at exacerbating pre-existing divides and frictions in a targeted community by combining – creatively and opportunistically – social and cognitive hacking, digital disinformation and fakes, sock-puppetry, bots, trolling and further techniques. The use of the cited techniques was especially noticeable during the US presidential election, but also during elections in Europe (including the referendum on Brexit) (Baezner and Robin, 2017). It is expected for other forthcoming electoral terms, when not only foreign States or their proxies but also domestic entities (radical groups or other organisations) are likely to engage in to deceptive influence.[26] Resort to these techniques is also traceable to different non-election-related operations run in Western Countries, the Nordic-Baltic region and Eastern Europe (Helmus et al., 2018; "Lisa Case" in NATO Review Magazine, 2016). Pending the outcomes of the on-going investigation, the Twitter campaign against the Italian President could be seen as a social media influence activity both employing and pursuing polarisation.

Again, some of the cited techniques integrate a certain degree of automation. Bots (especially spammer and impersonator bots) mimic organic behaviour to mislead, confuse and influence the users. Also known as social bots, they are commonly used to engage with political content on social media platforms. They are "highly efficient for amassing virtual social capital online to exploit social pressures and cognitive biases by acting as force multipliers, or false amplifiers in online discussions. Depending on the level of sophistication of a bot, this can be done by, for example, automatically following, re-tweeting, or liking posts from real social media accounts to boost their legitimacy, using spammer bots to reinforce impersonator bots, or using bots to crowd out dissenting opinions to create a false sense of consensus. Bots can repeatedly post and reinforce specific messages via multiple accounts and exploit features such as tags and hashtags to effectively direct content on

[25]In contrast to strategy as a more neutral term, stratagem invokes the meaning of trickery, of outwitting an adversary.

[26] Recently, Denmark has adopted an Action Plan to counter influence campaigns especially in view of the upcoming 2019 parliamentary elections. See Ministry of Foreign Affairs of Denmark, "Strengthened safeguards against foreign influence on Danish elections and democracy", 07.09.2018, accessed 24 September 2018 at http://um.dk/en/news/NewsDisplayPage/?newsID=1DF5ADBB-D1DF-402B-B9AC-57FD4485FFA4. Also, Canada next electoral term is at risk of influence: Communication Security Establishment, "Cyber Threats to Canada Democratic Process", 2018, accessed 24 September 2018 at https://www.cse-cst.gc.ca/en/democratic-process-processus-democratique/table.

social media platforms" (Pamment, Nothhaft, Agardh-Twetman, and Fjällhed, 2018, p. 57). Similar to bots are sock-puppets, which are not entirely automated, but partially controlled by a human. Semi-automated sock-puppets grant control over multiple false accounts to coordinate content across different community groups and platforms. (Pamment, Nothhaft, Agardh-Twetman, and Fjällhed, 2018, p. 58)

While social bots prove to be efficient tools for engaging in social media influence, they are also vulnerable to exposure. The same goes for other techniques listed above, like sock-puppeting, trolling, or hacking via dark advertisement. In principle, it is possible to detect when they are deployed and check if/how they are used within the scope of an influence operation. There are some methods proving to be useful in that regard.[27] The presence of some (often ambiguous!) indicators can raise a flag; further investigation and analysis would provide the necessary evidence. In general, if properly monitored, social media data offer a certain insight in to influence activities. They deliver information that, if analysed and further combined with other intelligence, can support detection and allow for counteraction. This should not bring to the conclusion that influence operations are easy to spot, especially at their early stage of preparation or enactment. They could be more easily recognised *ex-post*, *i.e.* after their execution. However, *ex-ante* or *interim* detection is in principle possible through the adoption of a social-media and multi-source intelligence-based approach.

Crafting Intelligence on social media influence operations

Ideal standards vs real constraints

Necessary but not sufficient conditions for countering social media influence are to understand these types of operations and being able to recognise them. Intelligence capabilities can play a significant role in this regard (Treverton, 2017, p. 21). Broadly speaking, they can be deployed by an organisation to collect and analyse social media data as well as other – both openly and covertly sourced – information in order to generate actionable knowledge of potential and actual illegitimate influence actions. To a certain

[27] Social bot detection is premised upon various approaches, which alternate or combine human engagement or algorithmic analysis. Crowdsourcing, social graph analysis, feature analysis are approaches which can be used alone or combined to detect a social bot. *Cf.* Marc-André Kaufhold and Christian Reuter, "Cultural Violence and Peace in Social Media: Interventions by Human and Social Bots", Conference Paper, Cyber-security Conference, Zurich 27-28 September 2018, to be published in proceedings.

extent, the (counter-) intelligence gathering activities aimed at understanding/recognising influence operations mirror those promoted by malevolent actors while preparing and planning for them. They share similar goals (*e.g.* mapping vulnerabilities and potentially targeted groups), sources (*i.e.* social and other media), collection tools (*e.g.* collection of data via bots), and analytical techniques (*e.g.* social network analysis) as well as they face analogous technical constraints. The most evident difference between the two "types" of activities lies in the decision-making-related purpose they aim to serve: influence and counter-influence. Other differences might concern both the technical and non-technical aspects of the intelligence gathering activities.[28]

In principle, intelligence on social media influence should cover the strategic, tactical and operational dimensions of these types of operations.[29] It should be crafted by processing data from social media and other sources of information with appropriate methodologies and tools. It should cover "introspectively" the relevant exploitable vulnerabilities and targets, but also address the "external" threat environment, like actors (both foreign and domestic), their capabilities and modus operandi.[30] Most importantly, it should be actionable *i.e.* afford ground for counter action. The normative nature of the above statements is evident. They suggest what intelligence on social media influence operations should look like. They portray an ideal of intelligence that clashes with what it is often possible to achieve in reality. Indeed, crafting high valuable intelligence on influence operations is a complicated task which requires the allocation of specific resources (human, technological, organisational). Furthermore, the intelligence production process itself is somewhat flawed. It is affected by the general and endemic limitations concerning the crafting of social media and cyber-intelligence (Bonfanti, 2015, pp. 231-262; Omand, Bartlet and Miller, 2012; Bonfanti, , 2018, pp. 105-121).[31] Among the main flaws lie the uncertainty, volatility, scale and anonymity of the data and the sources to be processed (information anarchy). These flaws give to the produced intelligence a high probabilistic connotation, which will in turn affect the scope, nature and effectiveness of possible counterinfluence actions.

---

[28] For example, the actor who engages in counter-intelligence gathering has to circumscribe the scope and reach of the collection according to what is prescribed by law, including privacy and data protection regulations.

[29] There is no clear demarcation from one level to another; they frequently overlap or are combined.

[30] It should adhere to the adage "know other and yourself".

[31] The space limitation of the present contribution does not allow a detailed discussion of the social media intelligence crafting process and it main constrains.

A (rough) cuboid representation of Intelligence on social media influence

In light of what has been discussed so far, intelligence on social media influence can be represented through the following cuboid model (Figure 1). Far for being a comprehensive representation of this type of knowledge, the model tries to capture its main ideal features.

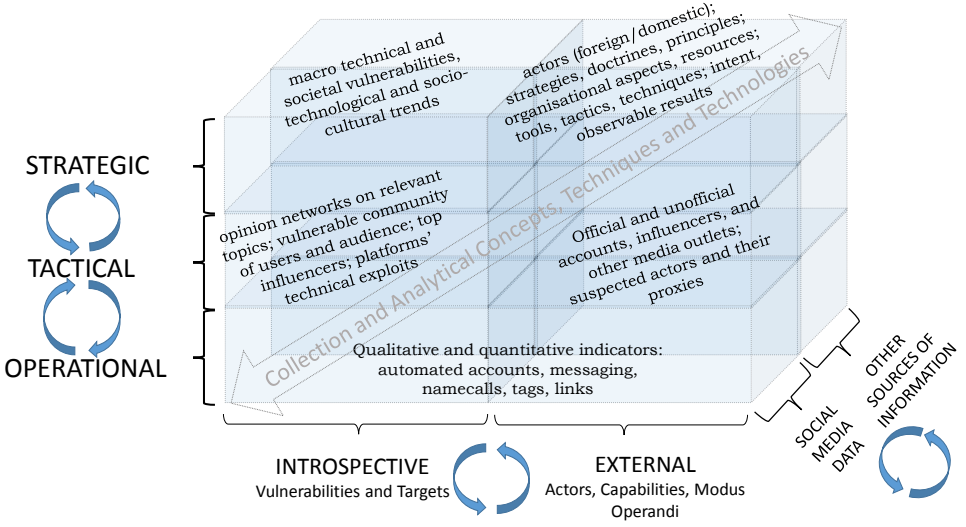


Figure 1: (Counter) Intelligence on Social Media Influence Activities

At the strategic level, intelligence on social media influence should provide insight into present and future threats as well as the risks associated with those threats. It should cover and review the threat landscape for macro trends and identify key threat actors, their goals, capabilities and how these may evolve in the mid-long term (Lin, 2018).[32] Strategic intelligence is generally rich in contextual information. Although focused on social media related influence, it may also frame these operations within broader cyber-persuasion or inform and influence operations and campaigns. With regard to social media, it can examine the actors (foreign or domestic) capable of

[32]As suggested by the author, one element of detecting influence operation is "recognizing parties that might have something to gain from conducting such campaigns. Mere recognition of who gains is not evidence that a party is undertaking an Information warfare and Influence campaign, but a party that does not stand to gain from such a campaign is unlikely to be involved in one".

engaging in to this type of influence, the strategies, doctrines and principles to which current operations are informed, the organisational aspects involved, and resources needed for running these operations, the tools, tactics and techniques they employ, their intent and observable results. Such strategic intelligence can derive from multiple sources. It can also derive from the collection, documentation and analysis of past cases and events.[33] Cases-analysis supports patterns recognition and assist in speculating on future developments or scenarios. Quite important, strategic intelligence should also address context-specific exploitable vulnerabilities and potential targets of social media influence. As discussed above, vulnerabilities lie in the platforms' design and functions, in the community of users, but also in the society as a whole. In a strategic perspective, these latter and the wider-technical ones are the most relevant. Societal vulnerabilities represent those which become also evident in domestic open debates. Most likely, they will be the ones at risk of exploitation from malevolent actors. In monitoring vulnerabilities and potential targets, technological, cultural and socio-economic trends should possibly be considered in order to foresee new potential opportunities for exploiters. Strategic intelligence generally serves apical decision-making processes aimed at achieving an organization's mission and determining its direction and objectives. It can for example support the definition of counter programmes adopted at the policy and legislative level.

At the tactical level, intelligence should concern what happens on selected social media platforms and, to a certain, extent, beyond them. It should be based on the monitoring of selected social media content (data and metadata), their communities of users as well as other online sources like blogs and webpages. With regard to social media, monitoring implies the processing of information which can be further analysed to: mapping opinion networks based on relevant discussion topics; circumscribing community of users and audience which are potentially exposed to influence attempts; identifying top influencers for each community and topics; charting platforms technical exploits. It also entails screening targeted on-line official or unofficial accounts or pages which can fuel influence operations. Information collection and analysis should occur according to pre-defined methodologies; they could benefit from automated or semiautomatic technologies and techniques.[34] With regard to automatic or semiautomatic collection, this task can be carried out

[33] The list of social media influence tools, techniques and stratagem examined above drew on analysis of both the literature and past events.

[34] Both the degree of automation and effectivity of technical collection and analysis could probably improve by the adoption of artificial intelligence-based solutions.

through: software applications designed for retrieving structured set of information from social media "Application Programming Interface (API)" (for example, Facebook Graph API, Twitter Search API);[35] other "scrapers", "crawlers", "spiders" as well as additional tools and algorithms that gather data and metadata to map the information environment of social media platforms; solicited/crowd source information to sense users sentiments. As per the analysis, concepts and approaches may vary. They may include: social network analysis, which involves identifying and visualising social structures and detect communities in large social media data; lexical analysis, to detect structures and patterns in textual data; sentiment analysis, providing insight in to community of users' attitudes, values, feelings; geolocation and geoinferencing, that are methods for determining the geographic origin of a social media messages and making inferences about the geographic location of posts; deep neural networks, to categorise images (Marcellino, Smith, Paul, and Skrabala, 2017). These analytical concepts are then translated into practical approaches and applications like, publics analysis, stance analysis, network description (Marcellino, Smith, Paul, and Skrabala, 2017, pp. 30-35).[36] Overall, they are part of the toolboxes used by different type of actors to generate the so-called social media intelligence (Bonfanti, 2015, p. 241; Omand *et alii*, 2012, p. 15). As mentioned above, the cited approaches, techniques and their application face specific limitations (technical, technological, legal) whose reach should not be underestimated both by those who adopt them to craft intelligence and by the consumer of such product (Bonfanti, 2015, p. 239). Tactically, intelligence on social media operations should also cover blogs, webpages or other on-line media outlets which are potential vehicles of influence. These should be mapped and monitored. The same goes for "off-line" actors like suspected domestic proxies of foreign entities which might fund and sponsor influence operations, or offer other kind of support to domestic actors. Generally more technical in nature, tactical intelligence on social media influence informs the steps and actions an organization can take to design and run counter measures.

Finally, operational intelligence should address imminent or initiated influence operations that pose an actual threat. Drawing upon the knowledge generated at the strategic and tactical level, this intelligence should aim at enabling short-term response, especially on the informative level (shut down

[35] Among this information, the geo-temporal coordinates of the users, the number of their information they generate and share, determine the number of their connections.

[36] Another approach is resonance analysis, which can be applied to measure the spread of specific information and narratives across a social media and identify communities of users. *Cf*. p. 47 ff.

malicious accounts, disseminate counter narratives). It relies on quantitative and qualitative indicators which can raise a flag on an occurring or started-up influence operation. From this point of view, social media enable to listen for malevolent activities by monitoring: accounts, messaging, tags, name calls, links, and attachments. At the very practical level, recognising entails detecting and identifying the tell-tale signs of a planned, ongoing, or concluded influence operations through social media. "The rapid emergence of large numbers of automated social chat bots promulgating similar messages could signal the start of a concerted operation, as automated chat bots do nothing but amplify discourse rather than contributing new content. More generally, one might imagine that some combination of volume (messages per day), content, and platform and so on could identify with probability automated social bots carrying divisive or inflammatory messaging" (Lin, 2018). Event detection or situational awareness techniques can prove to be useful in this regard too). (Abdelhaq, Sengstock, and Gertz, 2013; Atefeh and Khreich, 2015, pp. 132-164) The above described operational intelligence can trigger the deployment of already designed counter measures by response agencies.

Regardless of any clear-cut demarcation between strategic/tactical/ operational intelligence on social media influence operations, the ability to gain knowledge that covers all these levels is paramount. Each level is dependent on and integrated to the others. They overall provide the necessary perspective to look at social media influence operations, and better support recognition and counteraction.

Conclusion

Social media are relatively new means of information and engagement. They are used by an increasing number of individuals and organisations for creating, sharing, and consuming information, establishing or developing social or other relationships among them, and participating in the on-line (and off-line) community life. Broadly speaking, they are defining a novel space of action whose boundaries are yet to be firmly established.

Among other things, social media have also become both the theatre of and the tool for running illegitimate (cyber-) influence operations. Detecting this type of operations and clearly distinguishing them from genuine political or social engagement and campaigns is tricky. Detection can be pursued through the adoption of an intelligence-based approach. An approach that promises benefits but has its own limitations, and whose adoption faces specific challenges – limitations also include legal constrains. With regard to the limitations and challenges, they generally concern: the collection and

analytical concepts and techniques to be employed for generating tactical/operational intelligence from social media data and further information; the definition of tailored frameworks and procedures to integrate the obtained knowledge with further information and intelligence; the acquisition and deployment of relevant intelligence capabilities (Bonfanti, 2018, pp. 116-117; Bonfanti, 2015).

As per the collection and analytical concepts and techniques, their reliability and effectiveness – in providing valid results – is flawed by the nature of the data they are applied to, *i.e.* social media and, in general, Internet data. The uncertainty, volatility, scales and anonymity of these data undermines the validity/representativeness of obtainable results. This gives to the produced intelligence a high probabilistic connotation, which will in turn affect the scope, nature and effectiveness of possible counterinfluence actions. Another issue concerns the integration of multi-sourced information and intelligence. Technically, consistent integration is difficult to achieve because of the format, nature, and grade of uncertainty of social media and other on-line information. On an organisational level, integration should be achieved within structured collaborative frameworks in which collectors and analysts work together on regular basis. Further research on the topic and more practice/experience can help in improving the approach. With regard to capabilities, the gathering of the above described multi-layers intelligence on social media influence operations requires an organisation to acquire and allocate specific human, technical, organisational, and financial resources. The acquisition and allocation of these resources should prove to be sustainable and assessed for the return they generate.

A final note: it seems that further cases of domestic non-state actors' engagement in social and other online media influence operations (*e.g.* the Twitter campaign against the Italian President) are to be expected in the future – this seems at least the perception of some academics and practitioners. The phenomenon should be monitored and investigated in order to allow more effective law enforcement and security response.

References:

1. Abdelhaq, Hamed, Sengstock, Christian, and Gertz, Michael, (2013), "EvenTweet: Online Localized Event Detection from Twitter", *Proceedings of the VLDB Endowment*, Vol. 6. No. 12, accessed 24 September 2018 at http://db.disi.unitn.eu/pages/VLDBProgram/pdf/demo/p809-abdelhaq.pdf.

2. Arquilla, John and Ronfeldt, David, (1997), "A New Epoch — and Spectrum — of Conflict", in John Arquilla, David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, CA: RAND Corporation, pp. 1-20.

3. Atefeh, Farzindar, and Khreich, Weal, (2015), "A Survey of Techniques for Event Detection in Twitter", *Computational Intelligence*, Vol. 31, No. 1, pp. 132-164.

4. Baezner, Marie, and Robin, Patrice, (2017), "Cyber and Information Warfare in elections in Europe", Hotspot Analysis 2017, accessed 24 September 2018 at http://www.css.ethz.ch/publikationen/risk-and-resilience-reports/details.html?id=/c/y/b/e/cyber_and_information_warfare_in_electio.

5. BBC News, "Cambridge Analytica: The data firm's global influence", accessed 24 September 2018 at https://www.bbc.com/news/world-43476762.

6. Bonfanti, Matteo E., (2015), "Social media intelligence a salvaguardia dell'interesse nazionale. Limiti e opportunità di una pratica da sviluppare", in U. Gori, L. Martino (Ed), "Intelligence e Interesse Nazionale", Roma: Aracne Editrice, pp. 231-262.

7. Bonfanti, Matteo E., (2018), "Cyber Intelligence: In Pursuit of a Better Understanding for an Emerging Practice", *INSS Cyber, Intelligence, and Security*, Vol. 2, No. 1, pp. 105-121.

8. Brangetto, Pascal, Veenendaal, Matthijs A., (2016), "Influence Cyber Operations: The Use of Cyberattacks in support of Influence operations", in N. Pissanidis, H. Rõigas, M. Veenendaal (Eds.) 8th *International Conference on Cyber Conflict Cyber Power*, Tallinn: NATO CCD COE Publications.

9. Communication Security Establishment, "Cyber Threats to Canada Democratic Process", 2018, accessed 24 September 2018 at https://www.cse-cst.gc.ca/en/democratic-process-processus-democratique/table.

10. Costello, Katherine, (2018), "Russia's Use of media and Information Operations in Turkey. Implications for the United States", Perspective, Santa Monica: RAND Corporation, 2018, accessed 15 September 2018 at https://www.rand.org/pubs/perspectives/PE278.html.

11. Durante, Massimo, (2017), *Ethics, Law and the Politics of Information,* Dordrecht: Springer, Ch. 2, pp. 21-37.

12. FireEye, (August, 2018), "Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East", Report accessed 24 September 2018 at https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html

13. Floridi, Luciano, (2010), *Information: A Very Short Introduction*, Oxford: Oxford University Press 2010, p. 3.

14. Fubini, Federico, (August 3, 2018), "Le manovre dei russi sul web e l'attacco coordinato a Mattarella. In 400 per l'attacco sull'impeachment", *Corriere della Sera*, accessed 24 September 2018 at https://www.corriere.it/politica/18_agosto_03/manovre-russi-web-c6e7d71e-9699-11e8-8193-b4632fd4d653.shtml.

15. Gibney, Elizabeth, (2018), "The scant science behind Cambridge Analytica's controversial marketing techniques. Nature peers into the evidence for 'psychographic targeting'", *Nature*, accessed 24 September 2018 at https://www.nature.com/articles/d41586-018-03880-4.

16. Giuffrida, Angela, Kirchgaessner, Stephanie and Henley, Jon, (May 27, 2018), "New elections loom in Italy amid calls for Mattarella to be impeached", *The Guardian*, accessed 24 September 2018 at https://www.theguardian.com/world/2018/may/27/italys-pm-designate-giuseppe-conte-fails-to-form-populist-government.

17. Helmus, Todd C., Bodine-Baron, Elizabeth, Radin, Andrew, Magnuson, Madeline, Mendelsohn, Joshua, Marcellino, William, Bega, Andriy, Winkelman, Zev, (2018), "Russian Social Media Influence. Understanding Russian Propaganda in Eastern Europe", Santa Monica: RAND Corporation, 2018), accessed 24 September 2018 at https://www.rand.org/pubs/research_reports/RR2237.html.

18. Hornbuckle, Rob, (2016), "Social Media Vulnerabilities and Considerations for the Corporate Environment", accessed 24 September 2018 at http://www.infosecwriters.com/Papers/RHornbuckle_Social_Media.pdf.

19. Kaufhold, Marc-André and Reuter, Christian, (2018), "Cultural Violence and Peace in Social Media: Interventions by Human and Social Bots", Conference Paper, Cyber-security Conference, Zurich 27-28 September 2018, to be published in proceedings.

20. Lin, Herb, (2018), "Developing Responses to Cyber-Enabled Information Warfare and Influence Operations", *Lawfare*, accessed 24 September 2018 at https://www.lawfareblog.com/developing-responses-cyber-enabled-information-warfare-and-influence-operations.

21. "Lisa case" NATO Review Magazine, "The "Lisa case": Germany as a target of Russian disinformation", accessed 24 September 2018 at https://www.nato.int/docu/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm.

22. Marcellino, William, Smith, Meagan L., Paul, Christopher, Skrabala, Lauren, (2017), "Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations", Santa Monica: RAND Corporation, accessed 24 September 2018 at https://www.rand.org/pubs/research_reports/RR1742.html.

23. Ministry of Foreign Affairs of Denmark, "Strengthened safeguards against foreign influence on Danish elections and democracy", 07.09.2018, accessed 24 September 2018 at http://um.dk/en/news/NewsDisplayPage/?newsID=1DF5ADBB-D1DF-402B-B9AC-57FD4485FFA4.

24. Omand, David, Bartlet, Jamie and Miller, Carl, (2012), "#Intelligence", London: Demos Publishing.

25. Palmertz, Bjorn, (2017), "Theoretical foundations of influence operations: a review of relevant psychological research", accessed 24 September 2018 at https://www.msb.se/Upload/Om%20MSB/Forskning/Kunskapsoversikt/Theoretical%20foundations%20of%20influence%20operations.pdf.

26. Pamment, James, Nothhaft, Howard, Agardh-Twetman, Henrik, Fjällhed, Alicia, (2018), "Countering Information Influence Activities. The State of the Art", pp. 20-21, accessed 24 September 2018 at https://www.msb.se/RibData/Filer/pdf/28697.pdf.

27. Riformato, Serena, (May 27, 2018), "Governo, firme e tweet di solidarietà a Mattarella. Ma spuntano anche minacce di morte", *Repubblica*, accessed 24 September 2018 at https://www.repubblica.it/politica/2018/05/27/news/governo_dopo_le_minacce_di_impeachment_sui_social_parte_la_solidarieta_a_mattarella-197516727/.

28. Roeder, Oliver, (2018), "Why We're Sharing 3 Million Russian Troll Tweets", *FiveThirtyEight*, accessed 24 September 2018 at https://fivethirtyeight.com/features/why-were-sharing-3-million-russian-troll-tweets/.

29. Sarzanini, Fiorenza, (August 5, 2018), "Quirinale, dallo «snodo» di Milano l'account falso per l'attacco web a Mattarella", *Corriere della Sera*, accessed 24 September 2018 at https://roma.corriere.it/notizie/cronaca/18_agosto_05/dallo-snodo-milano-primo-account-falsoper-l-attacco-web-colle-5af8332e-98eb-11e8-9116-c731a1e8fd65.shtml.

30. Szafranski, Richard, (1997), "Neocortocal Warfare? The Acme of Skill", in John Arquilla, David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, CA: RAND Corporation, pp 395-416.

31. Treverton, Greg, (2017), "Influence Operations and the Intelligence/Policy Challenges", (Stockholm: Swedish Defence University – Centre for Asymmetric Threat Studies, 2017). p. 21, accessed 24 September 2018 at https://www.fhs.se/download/18.1ee9003b162cad2caa5351cf/1524483543405/Influence%20Operations%20and%20the%20Intelligence%20Policy%20Challenges.pdf.

32. Wüest, Candid, (2010) "The Risks of Social Networking", accessed 24 September 2018 at https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf.

INTELLIGENCE IN THE 21ST CENTURY

THE DESTABILIZATION OF DEMOCRACIES THROUGH THE SPREAD OF DISINFORMATION: THE ROLE OF INTELLIGENCE

Fernando VELASCO*
José Ángel GONZÁLEZ*

Motto: *No one dies of fatal truths nowadays: there are too many antidotes.*
Friedrich Nietzsche, "Human, All Too Human"

Abstract

Internet may be the most relevant development of our times, but together with its many benefits it has brought new challenges. One of them is disinformation or the so-called "fake news". This challenge should be approached both from an ethical and a technological perspective. Internet gives us access to a big amount of data but not all of it is true or valid, neither knowing the data is the same as understanding. Citizens are eager for information, but lies are more attractive than truths – generally considered as overrated – and whistle-blowers and social networks seem to be the only trustworthy sources. As a result, citizens – mainly the younger – are critically exposed to disinformation agents that sometimes even participate in disinformation networks organized at a State level in the battle for information; which poses a great risk for our democracies. A great problem to tackle this is the confrontation of legal measures to control profit-guided Social Networks and the persistence of basic principles for the EU such as the freedom of expression. The most effective way to face disinformation not falling under censorship must therefore be educating in critical thinking, and this means educating citizens in Intelligence Analysis.

Key words: *Disinformation, Intelligence Analysis, Critical Thinking education*.

* Professor PhD at Rey Juan Carlos University (Spain), Chief Director at the Centre for Intelligence Services and Democratic Systems (Cátedra de Servicios de Inteligencia y Sistemas Democráticos) and Co-Director of the Interuniversity Master Degree in Intelligence Analysis.

* MSc. Collaborator at the Centre for Intelligence Services and Democratic Systems and professor at the Interuniversity Master Degree in Intelligence Analysis.

Contextualization: internet, information and disinformation

I'm in Internet, therefore I am. Internet is, without a doubt, an achievement that has supposed a changing of era. It has many positive effects: never before so many citizens had access to such an amount of information as Internet offers, thus empowering transparency, supporting innovation, serving as a tool denouncing of abuses for the defence of citizens' rights and liberties. New technologies also make our daily lives easier. But on the other hand, just like the Roman god Janus, it also has a negative side that produces insecurities and new risks, summed to its rapid power of propagation. It gives us access to information in real time but at the same time its speed makes us forget it very quickly.

In the new world of Internet, speed is above verification, thus lies can be easily spread in a short period of time reaching almost everyone. In addition, as a recent research on "fake news" undertaken by a MIT research group proves (Vosoughi, Roy, and Aral, 2018, pp. 1146-1151), we consume more false information than truths regardless of the media we use, the conclusion we make is that citizens nowadays are easy to manipulate and, therefore, democracy is at risk.

Even if social networks seem to be a tool for "participation", they can be also used for "control": how are citizens going to make correct decisions if they live in a distorted reality? The frontier between truths and lies is becoming thinner and more liquid every time, to the point that it is hard to distinguish reality from fiction. New technologies mingle what is real and what is virtual, making us live in parallel worlds at the same time, worlds which are full of noise as everyone has something to say in every issue, and the ignorant and grotesque opinions (sometimes even aggressive) have been elevated to the category of "normal".

There is one thing clear about Internet: it is seducing. Social networks profiles keep growing as the anthem of our days seems to be "I'm in Internet – I'm an influencer –, therefore I am". Internet is nowadays the battleground of ideas, consequently also of lies and disinformation. But these new forms of communication only include those who think like one does, therefore debate is absent in the Net. This is the way how a great platform for the freedom of expression is becoming more and more of a "monitored liberty". We haven't doubt for a moment – what is worrying – to give up our privacy in order to gain "security" through new technologies, but at the same time, these new technologies have generated new tools to attempt against our privacy or damage our image, becoming so sophisticated that it is hard to detect falsifications (the so called "deep fake" or perfect falsifications). The use of

such disinformation techniques is both present at the personal level as it is in politics, business and international relations, where it poses a great risk for democracies. Indeed, we must be aware of how these tools weren't created to consolidate or potentiate democratic values, neither to educate well-informed citizens with a critical thinking. Furthermore, is anyone naïve enough to believe that the many researches on "fake news" financed by technological enterprises and investment funds will provoke a real Revolution? We are certainly allowed to "eat from all the trees in this Paradise" except from the one of critical thinking that would allow us to question the current dominant Model in the market for information. Personal data (tastes, interests…) have become a source of wealth, a precious asset for businesses and politicians, who with the help of algorithms and big data engineering are able to get to know us even better than ourselves. If you don't decide… they will do it for you. But what big companies such as Google, Facebook or Twitter know about us is simply what we have let them know. The massive use of our personal data in order to guide our decisions can be reflected in the words of R. Kapuscinski: "*The only player left at the world scene is multitude and its main feature is its anonymity, its lack of personality and identity. The individual has gone astray, has been diluted*".

Considering all this, in whom could we trust? Which institution has the moral authority and professionality to guide us away from disinformation? Where can we find impartial and rigorous information of quality? Whose analyses are yet trustworthy?

Disinformation: a threat for the European Union

Technology dependence on information gathering will not stop. The media on paper or those supported on non-mobile devices (television and others) will become extinct over time and give way to current (and new) devices and media that will allow a greater dissemination of ideas, concepts and opinions.

Given the global reach of information dissemination platforms, ideas, concepts and opinions will increasingly start from a greater number of sources, amplified by a greater number of comments and displayed on an even greater number of information platforms and devices. The linearity or exponentiation in diffusion will depend on the news interest to the public. Even in adequate news and well-intentioned writers, the constant flow of information between different groups of persons undoubtedly influences the noise on the channel, transforming the information as it passes from hand to hand. This fact, which has generated a moderate risk for mistakes by well-

intentioned journalists, has become a threat through polarized political discourse, headlines aimed at "click-bait" actions and reaching high-risk forms such as states or local groups that, through the use of these media, undermine European discourse and/or political processes in Europe. Disinformation, used against the interests of a nation, is clearly defined by the European Union: "*disinformation [...] we define it as false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit.*" (De Cock Buning, et al., 2018,) Disinformation generators can also analyse the population reaction to their information, modulating each message to implant their narrative in the population.

One of the bases of civilization is information. A civilization that is evolving more and more towards automation is based on information about the reality of its decision making, both for the optimization of its industrial, operational and organizational processes and for its management through the models of justice and equality on which the legislative system of the European Union is based. The decisions to be taken to improve and optimize any legislative process or base (from industrial processes to the adaptation of laws) must be based on a precise knowledge of reality, precisely the key factor that disinformation tries to attack, thus creating a distance between the different perceptions of reality: the "real" reality, the imagined reality (the reality perceived by the citizen) and the symbolic reality (which corresponds to the social and legislative model) (Johnston, 2018). Disinformation generates dystopia in the minds of citizens, separating reality from the result of its perception and distorting the credibility of the social and legislative model.

By adding to the actions of disinformation the lack of training from citizens to defend themselves, together with the lack of correct and abundant information on the part of the State and other social and journalistic groups, disinformation achieves its objective: citizen's incorrect decision-making based on false premises, manipulated and not corresponding to the imagined reality, according to Lacan's theory and directly related to Locke's epistemology, which is built around a strict distinction between knowledge and mere probable opinion or belief (Priselac, 2015). Citizens are eager for information and if the State and the media do not inform citizens truthfully and critically, others will do so, without so much truthfulness and based on their own agenda and interests.

Disinformation is not only located on websites – the classic web information manager on the Internet –, but it also accompanies citizens horizontally along all the platforms they use, mainly on mobile devices: from specific groups in Telegram to users of micro-blogging networks (Twitter), even helping some citizens to "jump and cross" information between different

networks, transferring information from one "app" to another. It is well known the influence that ISIS developed in some young people through videos aimed at lists of users of the mobile application Telegram (Kumar, 2017), channels also used by some intelligence agencies as a platform for Cyber-attack against their users (Dearden, 2018).

Platforms such as Telegram, Twitter, WhatsApp and the like have a differentiating factor that is the persistence of the information. Although these networks allow messages to be erased after reading, this ability is rarely used because what is intended is the persistence and archiving of messages to reach a higher level of capillarisation, through the sharing of content from a user to other related.

One of the advantages of the ability to analyse disinformation is its persistence, allowing the establishment of processes of historical analysis (and even post-Morten) of certain sources of information. Probably in the immediate future we will see how other social media that do not maintain persistence of the news and that are very demanded by young people are the media that disseminate disinformation (Snapchat and others), given its massive distribution content and inability to check "persistent" content. This fact is not taken into account by some studies (Fletcher*, et. al*., 2018) and would turn critical.

Given that the Internet Companies main objective in maintaining social networks is profitability, it is very difficult to prevent them from being open to anonymous publication, especially through false users or unidentified users, as the value of their networks rely on content. Although some of them indicate that they implement a code of practice, it is literally impossible by non-automated processes to evaluate the validity of the contents: Facebook receives on average 350 M of photographs each day, almost 2.5 M of photos per second (Aslam, 2018; Smith, 2018). Networks like Facebook and Google are working on Artificial Intelligence engines for automatic validations, but there are still years of development, training and debugging.

Given that the vast majority of information platforms and social networks on the Internet are in private hands, the European Union should (as a measure of legitimate defence) regulate the dissemination of this type of news through the existing legal model, respecting its bases and fundamental rights (such as freedom of expression) but establishing models of identification and defence against disinformation (Smith, 2018).

Near future technology will allow a greater expansion of disinformation, facilitating the generation of more sophisticated information creation and distribution. Work such as the one carried out at the University of Washington applying deep learning technology to video recordings, has

succeeded in supplanting the image of a person in a speech, thus allowing the transmission of a false video message that, in the eyes of non-experts, could be considered true (De Cock Buning, et al., 2018).

Fake news and ethics: blame it on the user?

An enemy of the people: fake news. H. Ibsen in his 1882 play "*An enemy of the People*" (Business Insider, 2017) already warned us how behind the appearances of truth and transparency, lies and manipulation are hidden. Just like the main character of the play, Doctor Stockmann, we have also discovered the lies that the waters of Internet drive through the spa of Internet and the risks its poses for democracy. If as citizens, we need to be properly informed in order to decide and make opinions, information is revealed as key. But when information is false or biased, then we have a problem. Experience taught us how the communication enterprises' interests few times if any take into account society general interest. In our case, the Spa is Internet and new technologies, therefore the Spa cannot be stopped.

Just like in Ibsen's play, we need to denounce how our society is democratic only in appearance because its citizens lack of their own opinion but also of the needed information to conform one. The author reminded us that the strongest man is that who defends truth even when in solitude.

In current times, the problem is maybe even more complicated. As McIntyre explains in his book "*Post-truth*", the problem with "fake news" is not merely that they expand false information, a phenomenon that, as he also analyses has occurred all along history. The real challenge of "fake news" is rather that they present themselves as deliberately false and have a clear final goal: political manipulation (McIntyre, 2018, p. 120). The task of Ibsen's "strong men" is no longer to unmask the lies hidden behind the appearance of truths, but to counteract information that is openly and publicly false and still has a greater impact and diffusion than true information. How can we defend ourselves form disinformation when truth seems to be no longer the matter of debate? This question takes us unavoidably to ask ourselves how we value truth in current times.

"Truth is overrated": the business of Lies. Mankind has had the general belief – standing still in our days – that "truth is overrated" and there is no special reason why we should give up lying if we become self-benefit or advantage from it. The only limit is therefore set by the possibility of being discovered. What is truly important is not if what I do or say is true or false, moral or immoral… but rather only if it is useful for our own self-interests.

Why should I – as a politician – take into account the truth if I have to win the elections? Or, why should I – as a businessman – take into account the truth when I have to close a deal or sell my product? Furthermore, what would really happen if all of us said only the truth?

These questions have been present in the writings of thinkers since the very beginning of the Western Civilization. Already Genesis (Chapter III, verse I) alerts us on how falsehood was present in the origin or the world: "*The man said: The woman you put here with me—she gave me some fruit from the tree, and I ate it. […] The woman said: The serpent deceived me, and I ate*." Maybe Paradise never existed; a place where truth, peace and kindness reign; a place previous to the appearance of lies.

Plato in his book "*The Republic*" (2005) deeply analysed the act of lying. Back at that time there was a successful doctrine called sophism. Sophists dedicated themselves to teach the young in the arts of persuasion. According to sophists, persuasion was necessary in order to progress and truth was not a requisite for the living. On the other hand, in Plato's opinion, sophism was a mean method as it took advantage of the ignorant. We should maybe ask ourselves who are the Sophists of our time.

On this line goes also the New Testament (Matthew, 7:15) when it advises us to take precautions and "*beware of false prophets, which come to you in sheep's clothing, but inwardly they are ravening wolves*".

Machiavelli's advice was rather different (probably, if he had lived nowadays he would have been quite an *influencer*). In his famous book "*The Prince*" he affirms that in order to acquire and retain power we need to be willing to do anything which is useful for it, regardless if it is moral or immoral, legal or illegal. In his words the Prince "*needn't be anxious about getting a bad reputation for vices without which it be hard for him to save his state: all things considered, there's always something that looks like virtue but would bring him to ruin if he adopted it, and something that looks like vice but would make him safe and prosperous*." (Machiavelli, p. 33) But we shouldn't take him wrong, as Machiavelli is only recognizing the use of lies, what has occurred as we analysed since the beginning of our times. He is putting us in front of the mirror. Also in Chapter XVIII he wonders about "How princes should keep their words". According to him "*Everyone knows that it is a fine thing for a prince to keep his word and to live with integrity rather than with cunning. But our recent experience has been that the princes who achieved great things haven't worried much about keeping their word. Knowing how to use cunning to outwit men, they have eventually overcome those who have behaved honestly*." Therefore, a Prince shouldn't keep his word when "*that could be used against him*". (Machiavelli, p. 37) This attitude is directly related to that of

appearances: "*But it's necessary to know how to camouflage this characteristic and to be a great pretender and dissembler*". Appearances are what define us. More important that telling the truth it is to appear to do so because, also in words of Machiavelli "*everyone sees what you appear to be, but few feel what you are*". (Machiavelli, p. 38)

Indeed, fiction has taken part – very efficiently – of our daily lives since the very beginning of our civilizations (mythology, fables, fairy tales…). Another clear example of it is religion, which still nowadays plays a key role in society. Fiction – and falsity – has the power to capture our attention, at least more than truth does. Y. Noah Harari in his book "*21 lessons for the XXI Century*" reminds us with humour how "*some fake news last only centuries*" (Harari, 2015, pp. 256-258). Maybe this was the reason why J.A. Comenio already considered in the XVII century that "*telling fairy tales and fables to children*" should be forbidden, as children "*would become used to taking lies for fun and they themselves would become used to lie as well*." (Sommer, 1995, pp. 198)

Similar to Comenio's was Paul Hönn (1622-1747) opinion regarding lies. The German jurist and writer accused in his "*Encyclopaedia of deception*" bakers of "*frequently and consciously buying old, staid and worms-eaten grain, which turns flour black and bad-tasting, only to sell it at the same price as bread of good quality*". Similar behaviour could be seen in shoemakers who sold old shoes at the price of new ones after they brightened them; as well as in tanners who "*sold goat leather as if it was mutton*" (Mendiola, 2006, p. 8). It would also be useful to ask ourselves if information is treated the same way as all these products.

Our society is still keener on impressions and appearances than in searching the truth. Maybe that was the reason why Nietzsche reminded us in his "*Human, All too Human*" preface how "*life has not been devised by morality: it wants deception, it lives on deception*" (Nietzsche, 1985). For many, governance and business are impossible without making use of lies; in other words, getting your hands dirty. Another philosopher, in this case Jean Paul Sartre, wrote about this concept in his play "*Dirty Hands*", in which one of its characters claims "*As for myself, my hands are dirty. I have plunged my arms up to the elbows in excrement and blood. And what else should one do? Do you suppose that it is possible to govern innocently?*" (Sartre, 1981) In other words, do you suppose that it is possible to always tell the truth? Isn't truth overrated? For the Prison Chaplain in Kafka's "*The Trial*" the answer to this question is pretty simple: "*No-said the priest- you don't need to accept everything as true, you only have to accept it as necessary*." To what the main character Joseph K. answers: "*A melancholy conclusion. It turns lying into a*

universal principle" (Kafka, 2013). But if we analyse it thoroughly, his words are not so melancholy. The "Order of Lies" in which we live has its advantages, and it may serve for a "Higher Truth". In word of Winston Churchill: *"In wartime, truth is so precious that she should always be attended by a bodyguard of lies".* The problem might arise when some States and politicians pretend to live in a constant State of War.

Similar to the fairy tales and fables we previously talked about, other doctrines such as marketing are also based upon fiction and lies. Creating a brand and making it relevant in the market requires to constantly repeating how drinking that drink, dressing those clothes, driving that car... would satisfy our needs. Not even mentioning the many cases of fraud, the task is to dilute the thin line between fiction and reality and one of the most effective tools to do so is lying. This is what we called the Business of Lies.

Even if the Oxford Dictionary declared in 2016 "post-truth" as the word of the year, we must affirm that we aren't living in a post-truth era, simply because there has never been a "truth golden era" either. Truth and Lies have coexisted since the very beginning of our times. Propaganda, deception, disinformation… they are all usual working tools. We have been taught that truth shouldn't interfere in the achievement of our interests.

Likewise, neither are Social Networks new phenomena. As Niall Ferguson reminded us in his book "*The Square and the Tower*" (Ferguson, 2018), all along history there have been networks pretending to control our data and information in order to retain the power. But we would be fooling ourselves if we didn't admit that never before have lies been so profitable as today. But, why? What is the difference? New technologies enable diffusion both to information creators and consumers. Lies have now a global projection through social networks: the effect of lying has become global. In words of Joseph Goebbels, Reich Minister of Propaganda at the Nazi Germany "*if you tell a lie big enough and keep repeating it, people will eventually come to believe it*". The biggest capacity to influence in others you have, the greater your power will be.

After this brief review there is one affirmation we can make to the point: firstly, we prefer lies to truths and truth is overrated; secondly, the road that takes us to power is constructed through hypocrisy and lies. In conclusion, truth and power don't go well together. If we want power, we will need to make use of lies, and if we want the truth we will need to give up power. Therefore, the question we all need to answer is the following: To whom do I serve… truth or power?

We would also be lying ourselves if we, after all the previous, considered that everything nowadays is false and that the bet for truth is a bet

for failure. Also, in the name of truth the worst actions against dignity have been committed, justified by many by considering truth as a metaphor of its times. Undoubtedly, Pilate's question is yet unanswered "*What is truth?*" (John, 18:38). In order to take the right decisions, we need to have rigorous and precise information. When reality is presented distorted to us, our decisions are determined by lies. How can we avoid false information and detect truth in the mess of Internet? How can we overcome the general believe that truth and facts have nothing to do with each other?

In Plato's "*The Republic*" (2005), there is an interesting myth for the current world we live: The Myth of Gyges. Gyges discovered a golden ring with which he became invisible. Using this power, he seduced the Queen, killed the King and so became the new Governor. What if we had a gadget that enabled us to spread fake news though Social Networks with the certainty of never being caught? Could we resist the temptation? Gyges couldn't.

The search for the Truth has been one of those values that has guided the Western civilization towards the noblest acts, giving meaning and a common goal to our history. We have reached a point at which we debate if the mere act of telling the truth is worth. Facts are no longer assumed as such due to objectivity, but rather because we agree with them or they emotionally move us. Everything is questionable and what we search in communication is no longer discussing with others but only reaffirming our ideas. But truth is different than that, because it inherently entails debate and contrast. In words of Antonio Machado the truth is "*not your truth: the truth. Come with me and we'll search for it. Yours, you can keep it for yourself*."

Disinformation agents. Blame it on the media?

But blaming it on the users alone wouldn't be missing a key factor in the equation of disinformation in Internet: the communication agents, the set of actors who must help citizens in the decision-making process based on rigorous information, formed by professional journalism at the service of society, together with Think Tanks, study centres and universities, all amalgamated with real information and analysis from the State. A model of truthful information generation will not leave space for disinformation generators, leaving their generators exposed to the informed citizen through their obviousness and shortcomings.

On the other hand, the 21st century's technological wealth (previously unthinkable) has facilitated the emergence of black swans from sources of information that, although reliable, have staggered states through the value of

the new information model based on the dissemination of restricted and secret information that has been filtered. Its maximum exponent is WikiLeaks.

Apart from the natural ethical, moral and national security considerations, the WikiLeaks model has impacted the entire chain of information generation and dissemination, modifying how citizens see their leaders and state, showing them that imagined reality (according to the Locke model) has nothing to do with symbolism. The model initiated by WikiLeaks has created a trend in almost the entire journalistic profession, with few media resisting to receive filtered information. In fact, prestigious media such as The Guardian facilitates anonymity through Tor network for anyone who wants to anonymously deliver filtered reports (*The Guardian*, 2018). This new vision of "obtaining information" according to the jargon of intelligence generates new challenges and approaches.

Among these risks are the strategic ones, based on internal leaks of confidential documents that could harm the European Union, to media "of low professional consideration" that prefer the exclusive news (ergo, increase in income) to the responsibility of the publication. In fact, the professionalism of the press saved in some ways the confidentiality (and their life in some cases) of those involved in the secret documents related to the Iraq war that Bradley Manning delivered to WikiLeaks, being sent before to a network of prestigious newspapers that processed the information received with a common criterion and responsibility, erasing critical information about persons and specific situations.

One fact worth reflecting on is the value and "respectability" of the media that filter information and how they are used for disinformation. After the WikiLeaks' information leak by Edward Snowden on the Internet and telephone interception systems in the USA, by Bradley Manning on Iraq, TTPA documents and Sony information among others, WikiLeaks achieved a very high prestige as a reliable source of information (without considering its moral and ethical values) according to the quality of the information they were delivering. When Hillary Clinton's email contents were illegally accessed and distributed, allegedly to destabilize the U.S. elections (Office of the Director of National Intelligence, 2017), the architect of this action used WikiLeaks with its "prestige" as a quality informant and with the necessary impact capacity on content dissemination across the traditional media, turning WikiLeaks into a pawn at the service of manipulation and information war and undermining its previous reputation.

Another fact that we must consider – especially after seeing the impact that secret information such as the one distributed by WikiLeaks – can affect and destabilize a State, is the level of information that the European Union

publishes about its operation. There is no doubt that it is a fundamental right of the European citizens to know the operations, forecasts and strategies of the European Union (such as those found at http://www.europa.eu), but this information could be used (and in fact it is) by third countries as an aid in their intelligence analysis for the establishment of their global strategies, in which the EU is one more element to take into account. Once again it is necessary to establish a balance between the right to know of EU citizens and the dissemination of information.

Attacks on society based on information

Civil society is the new target of disinformation. And disinformation should not be combated by a one-dimensional approach, as the message conveyed and its technique encompasses multiple dimensions (De Cock Buning, et al., 2018).

Citizens are much more exposed actually to news that they were in the pre-Internet and pre-Mobile era. Young generations, under the paradigm Information, Advice and Guidance (IAG), base their judgment and knowledge on information directly obtained from Internet (Healey, 2014). As disinformation spread is interlinked directly with the development of digital media (De Cock Buning, et al., 2018), we can conclude that new generations are directly exposed to the levels of disinformation present on social media, one of the main instruments used for information, advice and guidance, in their decision-taking processes.

Digital media and its exponential growth have also enabled the production and circulation of disinformation with a wider and easy reach, on a larger scale than previously, often in new ways that are still poorly mapped and understood (Fletcher, *et.al*., 2018).

As new technologies are deployed, new techniques, procedures and methods should be developed. As an example of this fact, in 2014 three authors from the Republic of Belarus wrote for Russia's journal Vestnik Akademii Voyennykh Nauk (Journal of the Academy of Military Sciences), an article in which exposed that the military must train specialists who were prepared not only for armed conflict but also for information-psychological and other new-generation warfare, including psychological warfare (Kuleshov, et.al., 2014, pp. 104–109). The same article describes targets and narratives identified in information campaigns, developing the following ideas:

"*To win an information-psychological confrontation, a belligerent must:*

- *change citizens' traditional moral values and 'landmarks', create a lack of spirituality, and cultivate a negative attitude towards one's cultural legacy;*

- *manipulate the consciousness of social groups by implementing so-called 'democratic transformations';*
- *disorganise state administrative systems;*
- *destabilise political relations among parties and coalitions to provoke conflicts and distrust; exacerbate political struggles and provoke repression against the opposition;*
- *reduce the level of information support for organs of authority;*
- *misinform the population about the work of state organs;*
- *provoke social, political, national, and religious conflicts;*
- *mobilise protests and incendiary strikes, mass disorder, and other economic protests;*
- *undermine the international authority of a state; and*
- *damage important interests of a state in the political, economic, defence, and other spheres."* (Kuleshov, et.al., 2014, pp. 104–109)

Targeting audiences

Disinformation-generating agents are continuously adapting their message to target audiences. Countries that use disinformation at the state level are adapting to traditional and local languages as long as media for the geographical and cultural places to which they are directed:

- China: "*aimed at influencing and conditioning perceptions. It is conducted through television programmes, newspaper articles (particularly in China Daily and the Global Times), books, films, and the Internet, as well as through monitoring and censorship of social media networks and blogs such as Sina Weibo (China's equivalent of Twitter) by the Chinese Communist Party (CCP)'s 2 million official 'public opinion analysts'. China's extensive global media network, most notably the Xinhua News Agency and China Central Television (CCTV), also plays a key role, broadcasting in foreign languages and providing programming to stations throughout Africa, Central Asia, Europe, and Latin America."* (Jackson, 2015)
- Russia: "*Not surprisingly, the government in Moscow now controls the majority of television and print media in the country. The majority of television and print media in the country. Freedom House, an independent human rights watchdog organization, evaluated Russia's press status as 'not free' in 2014, citing a 'vast, state-owned media empire' and the consolidation of several national media outlets into one large, state-run organization, Rossiya Segodnya (Russia Today): The state owns, either directly or through proxies, all five of the major national television networks, as well as national radio networks, important national newspapers, and national news agencies. ... The*

state also controls more than 60 percent of the country's estimated 45,000 regional and local newspapers and periodicals. State-run television is the main news source for most Russians and generally serves as a propaganda tool of the government cal policy goals' in a 2014 Baltic News Service report. Moscow has exploited its nearly exclusive control over Russian-language information, investing heavily in its state-run media apparatus, including a 2015 budget of '15.38 billion roubles ($245 million) for its Russia Today television channel and 6.48 billion roubles ($103 million) for Rossiya Segodnya, the state news agency that includes Sputnik News,' the Guardian said. By saturating a market already devoid of moderate independent" (Cotter, 2016).

On the Internet, the information agencies of the respective countries have a presence in all the social networks with the greatest impact (Twitter, Facebook, Instagram, Snapchat...) as an amplifier of the information generated from traditional media.

Disinformation targeting population creates risks that include threats to "*democratic political processes, including integrity of elections, and to democratic values that shape public policies in a variety of sectors, such as health, science, finance and more.*" (De Cock Buning, et al., 2018)

The clearest example is the United States, which certifies the impact and possible turnaround in a democratic election carried out from an opposing country, with the aim of destabilizing its political class (Office of the Director of National Intelligence, 2017). The United States government study referred here ensures that "We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump:

- *"Russia's intelligence services conducted cyber operations against targets associated with the 2016 US presidential election, including targets associated with both major US political parties."*
- *"We (USA assess with high confidence that Russian military intelligence (General Staff Main Intelligence Directorate or GRU) used the Guccifer 2.0 persona and DCLeaks.com to release US victim data obtained in cyber operations publicly and in exclusives to media outlets and relayed material to WikiLeaks."*
- *"Russian intelligence obtained and maintained access to elements of multiple US state or local electoral boards. DHS assesses that the types of systems Russian actors targeted or compromised were not involved in vote tallying."*

- *"Russia's state-run propaganda machine contributed to the influence campaign by serving as a platform for Kremlin messaging to Russian and international audiences."* (Office of the Director of National Intelligence, 2017)

One of the key aspects of these activities is their defence capacity based on "plausible deniability": "*By their nature, Russian influence campaigns are multifaceted and designed to be deniable because they use a mix of agents of influence, cut outs, front organizations, and false-flag operations.*" (Office of the Director of National Intelligence, 2017)

On the other hand, countries such as Russia maintain in parallel to political and even military actions operations that could be qualified as information actions on the population of their areas of strategic interest, generating a narrative spread by means controlled by the State and directed to specific sectors of the population of those areas of interest to them: "*Putin has leveraged the fact that most Russian-language media available throughout the world is broadcast or rebroadcast directly from Russia, where the Kremlin maintains a tight grip on the media. This has created a series of exclusive narratives, carefully crafted to influence specific population groups, including those beyond the borders of Russia and eastern Ukraine.*" (Cotter, 2016)

Educating in critical thinking: Intelligence analysis

Through all the previous analysis we can conclude that the current challenge of "fake news" or disinformation in Internet cannot be approached from one perspective alone. Ethic and informatics (among so many other areas) must be combined in order to pose realistic solutions to this problem. Both the user – who discredits truth and is generally not properly trained to detect lies – and the communication agents – who have displayed targeting mechanisms and, in some countries, complex political and security strategies making use of disinformation – are to blame.

Good practices tend to fall into three major categories, transparency, trust-enhancement, and media and information literacy (De Cock Buning, et al., 2018), relying again on crucial EU's document, and in order to act against disinformation, the EU recommends activities in the following directions:

> *"1. Enhance transparency of online news, involving an adequate and privacy-compliant sharing of data about the systems that enable their circulation online;*
>
> *2. Promote media and information literacy to counter disinformation and help users navigate the digital media environment;*

3. Develop tools for empowering users and journalists to tackle disinformation and foster a positive engagement with fast-evolving information technologies;
4. Safeguard the diversity and sustainability of the European news media ecosystem;
5. Promote continued research on the impact of disinformation in Europe to evaluate the measures taken by different actors and constantly adjust the necessary responses.

The EU also advises to disregard other type of solutions that could even be simplistic given the complexity of the problem or relay on actions against EU regulations and spirit, as censorship, Internet fragmentation or any technological intervention on Internet's technology.

Other solutions according to EU spirit include *"Civil Society Actors and journalism-NGOs, fact-check and verification, consumer protection and media literacy training as watchdogs, as well as by holding political and economic powers accountable for their actions."*

A good starting point would be requesting big social networks such as Facebook, Twitter or Google to better self-regulate the spread of fake news, together with a better legislation on the matter from Governments and more self-responsibility from the users. But investing in the human factor through education reveals to us even more urgent. We need to educate citizens in critical thinking through the Intelligence Analysis if we don't want that democracy vanishes. But this task has many challenges: how do we transform digital citizens – conformist and easy to manipulate – into critical citizens?

One of the Internet traps in which we have felt is believing that knowing data was the same as understanding. However, we have become aware that knowing what is happening is not enough to really understand reality, we need to give a meaning to it. But analysing is not a common trend, but rather almost a revolutionary act.

Internet is like an "information tsunami" which drives us through an enormous amount of information, most of it being trivial, false and misleading. All we need to do is to separate from it the "drinking water" which is the analysed information, information that would enable us to understand reality and see beyond its surface. The victim drowning under these waters is no other than democracy. Technological advances such as internet or artificial intelligence seem useless when employed by non-critical and narrow-minded citizens who can't distinguish between opinion and information, marketing and product, propaganda and history, ideology and politics.

Being difficult in the world we live in to establish an authority, a guideline, a common standard to identify truth, is urgent to provide our

citizens – specially the youth – of analysis techniques and abilities so that they can effectively participate in democracy. To educate in and for critical thinking through intelligence analysis implies at least to make the following assumptions:

- Becoming aware of how without information, there is no freedom. Those who have no information can't chose, decide nor control. Considering that information is not entirely neutral and objective, we need to inculcate citizens in the ability to make judgements because not everything doesn't matter neither everything is valid.
- Acknowledging that there is no critical thinking without a critical attitude, which requires of being open minded, tolerant and to question evidences. The best breeding ground for critical thinking is no other than the one that exchanges cultural perspectives, dialogues at the border, boosts our curiosity and astonishment, stimulates confrontation and fosters hypothesizing. We need new ways of asking.
- Learning to act on the terms of problems: the language. Because there is great difference in the use of one words and others.
- Learning to demand our media something more than entertainment. Because we yet prefer quick and superficial messages.
- Being aware of how education goes further than teaching institutions.
- Learning to be realists and confront risks and their consequences to avoid them, assuming that the contact with reality cannot be undertaken through internet alone.
- Learning to analyse (doubt, criticize) everything, including the democratic system itself.
- Learning to assume each own's responsibilities, even when they are easily transferred to others
- Accepting that being properly informed has an economical cost and that free information can lead to confusion. Information should not only be contrasted but extended with specialized literature, and we should also investigate and consult new and different sources.
- Learning not to make simplistic judgements: good-bad; friends-enemies.
- Being aware of how fear is always used as a weapon of control.
- Acknowledging how, even if the world is complex and exact truth may not exist, even if probably no politician tells the truth as it is, there is a difference between a democrat and a dictator.
- Remembering how in the way towards truth "*wanderer, there is no path, the path is made by walking*" (Antonio Machado).

Of course, the Intelligence Services have also a task in this process and – through Intelligence Culture – they should become aware of how a well-informed and educated citizen is always a great ally.

In conclusion, educating in and for critical thinking through intelligence analysis is no other than educating in the responsibility for what is useful, being useful everything that makes us improve as a society. It is good to keep always in mind that is better to die for an unconquerable truth than living for a well-paid lie. At the end, what is at stake in both cases is each one's self.

From intentions to Actions: 2018 CSISD course, educating educators

Following the EU recommendations on its last proposal regarding disinformation we have mentioned all along the text and also according to the considerations mentioned above, the Centre for Intelligence Services and Democratic Systems (*Cátedra Servicios de Inteligencia y Sistemas Democráticos* or CSISD) with the support of the Rey Juan Carlos University at Madrid has recently developed and implemented a pilot course on Critical Thinking and Fake News together with the Autonomous Community of Madrid; directed to secondary grade teachers as a vehicle to reach a young population who, as we have mentioned several times, are the most vulnerable to disinformation and are the citizens upon which the future of our democracies rely.

The main goal of this course is to create a layer of secondary school teachers with specific capabilities and knowledge to introduce critical thinking and disinformation detection to their students, including new concepts and tools in the already existing educating programs and extending their teaching skills on concepts not included in educational planning.

CSISD developed a complete syllabus together with a teaching program based on disinformation identification training and Critical Thinking skills, including the following topics:

- Basic Concepts:
  - The need for knowledge in society: history and concepts;
  - Terminology;
  - Critical thinking;
  - How disinformation arises;
  - Digital contexts as support and dissemination of information;
  - Ethics and the media.
- Information: channels and dissemination:
  - The individual and information;

- Sources of information.

- Impact of false information or disinformation:
  - Personal opinion and decision making;
  - Importance of Information;
  - Targeted attacks based on false information;
  - Impact on society and democratic systems.

- Initiatives to counter false information and how to be protected against false information, disinformation and other attacks through information:
  - Detection;
  - Contrast and information environment;
  - Methods to counter disinformation and false information.

The results have been very positive and the teachers and schools involved are demanding for new courses which will be carried out in the near future, with the intention of setting a precedent and promoting similar trainings in other areas of Madrid and Spain.

References:

1. Aslam, S., (2018), *Snapchat by the Numbers: Stats, Demographics & Fun Facts. [Online], Omnicore*. Available at: https://www.omnicoreagency.com/snapchat-statistics/ [Accessed 27 Sept. 2018] See also Smith, C. (2018). 65 Amazing WhatsApp Statistics and Facts [online] Expanded ramblings. Available at: https://expandedramblings.com/index.php/whatsapp-statistics/.

2. Business Insider (2017). Researchers created fake footage of Obama speaking – and the results are scary. [Online], in *The Business Insider*. Available at: https://www.youtube.com/watch?v=3mNf1euL3vI.

3. Cotter, Brian P., Capt. U.S. Army (2016*), Russkiy Mir – How the Kremlin employs narratives to destabilize the Baltic States*, [online], Countering Russian Propaganda, *Per Concordiam. Journal of European Security and Defence Issues* - George C. Marshall European Centre for Security Studies. Available at: http://perconcordiam.com/perCon_V7SPED_ENG.pdf pp. 31-33.

4. Dearden, L., (2018), *Isis hit by onslaught of fake propaganda and cyberattacks*. [Online], in *The Independent*. Available at: https://www.independent.co.uk/news/world/middle-east/isis-islamic-state-propaganda- telegram-offical-fake-cyberattacks-accounts-a8442936.html.

5. De Cock Buning, M., *et al.* (2018), *"A multi-dimensional approach to disinformation"*. Report of the independent High level Group on fake news and online disinformation, [online] European Union, Available at: https://ec.europa.eu/digital-

single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

6. Ferguson, N., (2018), "*La plaza y la torre. Redes y poder: de los masones a Facebook*" Madrid, Editorial Debate.

7. Fletcher, Richard, Cornia, Alessio, Graves, Lucas, and Nielsen, Rasmus Kleis, (2018), *Measuring the Reach of 'Fake News' and Online Disinformation in Europe* [online] Oxford: Reuters Institute for the Study of Journalism, Available at: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2018-02/Measuring%20the%20reach%20of%20fake%20news%20and%20online%20distribution%20in%20Europe%20CORRECT%20FLAG.pdf.

8. Healey, Matthew, (2014), *An examination of the extent the internet has empowered young people to take greater control of their information, advice and guidance needs*, University of Southampton, School of Social Sciences, Doctoral Thesis, 372 pp.

9. Jackson, L., (2015), *Revisions of Reality the Three Warfares—China's New Way of War,* [online], in Legatum Institute, Beyond Propaganda – September 2015. Information at War: From China's Three Warfares to NATO's Narratives, Available at: https://lif.blob.core.windows.net/lif/docs/default-source/publications/information-at-war-from-china-s-three-warfares-to-nato-s-narratives-pdf.pdf?sfvrsn=2, p. 5.

10. Johnston, A., (2018), *Jacques Lacan* [online], "*The Stanford Encyclopedia of Philosophy*" (Fall 2018, Edition), Edward N. Zalta (ed.) Available at: https://plato.stanford.edu/archives/fall2018/entries/lacan/.

11. Kafka, F., (2013), "*El proceso*", Madrid, Alianza Editorial.

12. Kuleshov, Iu. E., B. B. Zhutdiev, B. B., Fedorov, D. A., (2014), *Informatsionno-psikhologicheskoe protivoborstvo v sovremennykh usloviyakh: teoriya I praktuka* ("Information-Psychological Confrontation under Contemporary Conditions: Theory and Practice"), Vestnik Akademii Voyennykh Nauk (Journal of the Academy of Military Science), pages 104–9.

13. Kumar, T., (2017), *Here's how ISIS Uses the Telegram App for Its Hateful Propaganda*, [Online], The Quint – Bloomberg. Available at: https://www.thequint.com/news/world/how-isis-uses-telegram-app-for-propaganda.

14. Machiavelli, N. (n.d.), "*The Prince*"; pp 33. Consulted online at the Early Modern Texts Library. Available at: http://www.earlymoderntexts.com/assets/pdfs/machiavelli1532.pdf

15. McIntyre, L., (2018), Posverdad. Madrid, Ediciones Cátedra.

16. Mendiola, I., (2006), "*Elogio de la Mentira: En torno a una Sociología de la Mendacidad*". Madrid, Lengua de Trapo.

17. Nietzsche, F., (1985), "*Humano, demasiado humano*", Madrid, Editorial Edaf.

18. Noah Harari, Y., (2015), "*21 lecciones para el S. XX*" Madrid, Editorial Debate.

19. Office of the Director of National Intelligence (2017), Background to 'Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution' – ICA 2017-01D, [online], Office of the

Director of the National Intelligence, United States of America, Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf.

20. Platón (2005), "*La República*". Madrid, Alianza Editorial.

21. Priselac, M., (2015).], *Locke: Knowledge of the External World* [online], Internet Encyclopaedia of Philosophy, University of Tennessee, available at: https://www.iep.utm.edu/locke-kn/.

22. Sartre, J.P., (1981), "*Las manos sucias*", Madrid, Alianza Editorial.

23. Smith, C., (2018), *65 Amazing WhatsApp Statistics and Facts* [online]. Available at: https://expandedramblings.com/index.php/whatsapp-statistics/.

24. Sommer, V., (1995), "*Elogio de la mentira*", Madrid, Galaxia Gutemberg.

25. *The Guardian*, (2018), *Share stories with us securely and confidentially* [online]. Available at: https://securedrop.theguardian.com/.

26. Vosoughi, S., Roy, D., Aral, S., (2018), "*The spread of true and false news online*". Science, Vol. 359, Issue 6380.

INTELLIGENCE AND COUNTERTERRORISM: THE MEANING OF WORDS IS THE RIGHT TOOL TO MAKE AN EFFICIENT ANALYSIS WHEN THE THREAT IS HYBRID

Sabrina MAGRIS[*], Martina GRASSI[*], Perla DI GIOIA[*]

Abstract

Intelligence makes errors because it does not know their meaning of words (DB psyops). Using words and understanding their meaning allows seeing the reality and distinguishing it from what is not real. As the terrorists who have committed the last terrorist attacks in Europe that, nowadays, we all called "radicalised" (extremist) but that cannot be radicalised.

It is scientifically impossible to define as "radicalized" a subject that becomes interested and gets close to religion practices all dogmas in a couple of months. The cognitive process -that allows to encode the information- needs time in order to permit the writing of neural cells in the brain (for instance, choosing to start the elementary school at five/six years it is not a random choice as at this age the areas of the child's brain are formed and ready to learn).

Numerous studies have proven that for a radicalised individual to actually change his/her behaviour and mind-set requires no less than 7-8 years, so that s/he can interiorise content, ways of thinking and elaborations. These individuals can be defined as "infatuated" and have different characteristics from those that a real radicalised individual would have, therefore also the security algorithms used to identify these individuals need to be based on different criteria otherwise they won't be able to early detect and identify the threat.

Keywords: *bias, i-bias, gathering information, overcoming bias, terrorism infatuated*.

[*] President of École Universitaire Internationale, Director of Research École Universiaire Internationale Rome – Italy, president@ecoleuniversitaireinternationale.net.

[*] Head of International Activities, Fellow Researcher, École Universitaire Internationale Rome – Italy, ia@ecoleuniversitaireinternationale.net

[*] Fellow Researcher, École Universitaire Internationale Rome – Italy, pdg@ecoleuniversitaire internationale.net

Introduction

This paper investigates biases linked to the intelligence work, specifically those who have been defined as I-BIAS (Magris, Grassi, 2018). It will analyse not only the biases that impede the intelligence practitioners to work at the best of his/her capabilities but it will also address and refer to various ways to overcome such biases. Specifically, this paper will analyse, amongst the I-BIAS, those physiological biases that affect the work and daily life of any human being, intelligence practitioners and analysts included. It will underline the macro and micro systemic dimension of psycho-social biases and how, working on those, it becomes easier to eliminate individuals' psycho-social biases.

Moreover, this paper will stress how those biases have sometimes mislead the intelligence in identifying the terrorists that have committed the recent terrorist attacks in Europe, and how an analysis based on the correct meaning of words would have led the intelligence practitioners and analysts to more effectively predict the threat and find solutions to prevent it.

Taking into account the intelligence failures of the past years caused by biased analysis, this paper will explain the differences between a radicalised individual and an 'infatuated' one, allowing the establishment of new parameters and features with which update the security algorithms in order to early identify individuals like those who have committed the recent terrorist attacks in Europe and those who might attack in the future.

Given the hybrid threats that threaten our society, intelligence practitioners must be able to use every abilities and resources they might have in the fastest way possible.

Bridging the gap between academia and practice, this paper specifically addresses what it has been defined as I-Bias – Intelligence Bias – biases linked to intelligence and intelligence practitioners.

What is written in this paper is the result of the paper's authors' researches and elaborations and of the École Universitaire Internationale research centre. The term I-BIAS (Magris, Grassi, 2018) indicates all of those errors of perception, errors of vision and culture that impede correct analysis, that slow down analysis or induce the practitioner to make mistakes both in the analysis and in the field work, creating research models based on basic errors.

Correcting these basic errors since their beginning leads to committing fewer errors, to higher chances to accomplish an operation and to remarkably decreasing economic costs and resources.

Why terrorists can easily travel across Europe, being inspected without being recognised as terrorists? Why did our intelligence know the

terrorists but it was not able to stop them before the attacks committed in the last years?

This is because the intelligence activity was biased. For instance *Salah Abdeslam,* the terrorist that made the attack against the *Bataclan* theatre in Paris in the 2015 was stopped in Italy by the Italian police force when he was driving in the north of Italy but he was not considered as a possible terroristic threat. After his failure, he committed the attack a few months later.

He was stopped while he was coming back from Syria by car. The policemen that stopped him did not consider the possibility to easily go from Belgium to Syria by car, crossing several states. And so they did not make the connection.

A wrongful view of terrorists leads to committing analysis errors. In this case, the police officers that stopped *Salah Abdeslam* checked only his documents but did not cross over information that was out in the open, and that would have risen doubts. For instance he was travelling on rented car with a non-Italian car plate perfectly in order that had crossed various borders from Belgium to Turkey.

In order to cross over and drive by many borders, it is necessary to buy specific stickers to stick to the car window. Analysing this, it would have been easy to infer the journey the individual had made and ask for more information. However, the limits imposed to the officers by their assignment, traffic control, prevent them from making a broader analysis.

Their analysis was biased. A bias is an "inclination or prejudice for or against one person or group, especially in a way considered to be unfair" (Oxford University Press, 2018). Bias is "the action of supporting or opposing a particular person or thing in an unfair way, because of allowing personal opinions to influence your judgement" (Cambridge, 2018). Therefore, bias is a cognitive error, an error of perception. Those errors misguide perceptions and analysis of situations, events, people and facts. Biases refer to attitudes or stereotypes that affect our understanding of actions and decisions, attitudes and beliefs about a person or a group or facts.

Biases affect one's daily life and work, as they become an obstacle to perceive reality as it is rather than what the individual wants it or thinks it to be. Bias can be caused by physical trauma (i.e. dysfunction, pathology), by culture, education, social influences, experiences. It is a distortion of the evaluation process. The major part of biases derives from psycho-social influences, particularly from the environmental and social influences – macro system. However, the individual develops numerous biases based on his own experiences such as family, relationships, school and friends – microsystem. The biases developed ~~on~~ by personal experiences tend to have a stronger

influence on the individual respect those from the outside of society, strongly affecting his thoughts and behaviours.

Working on eliminating biases, it is important to bear in mind to work on the elimination of both macro systemic and micro systemic biases in order to effectively eliminate the individual's biases. Working at the same time on the double binary (macro and micro) it becomes easier to find solutions to overcome and eliminate also psycho-social biases.

Besides psycho-social biases recent researches by École Universitaire Internationale discovered that there is also another type of bias: a physiological bias. It is the elaboration of internal or external information aimed to cover up what is missed of the real information. The brain creates an ostensible version of what happens -based on the information it has already stored, without codifying new information- because it does not have the reality of what happens.

At the neural level it indicates the deficiency of substances that enable the connections between the parts of the brain involved causing the non-codification of the information received (Bellomo, 2017).

There is a particular bias called change blindness (ICD-10-CM, 2018) that can be categorised as physiological bias. It can be a consequence of a physical or psychological trauma. It is a perceptual phenomenon that occurs when someone fails to see a change in what he is looking at, someone that does not see that something has changed.

An experiment conducted by Simons and Levin (1998) in the 90s shows precisely change blindness. It shows a man talking to a guy explaining him direction when, at some point, a couple of men pass by with a big cardboard hiding a different man who replaces the guy asking for direction. After the cardboard has passed the man continues to give direction without realising that the guy he is talking to is a completely different guy, dressed in a completely different way.

Even though Change blindness has been discovered years ago it still affects the all population, even intelligence practitioners. That is because it has never been looked for the specific biases that affect the intelligence practitioner—using/through specific tests aimed to evaluate the real practitioner reliability, such as the test realised and applied in the I-Bias studies. These tests can be conducted since the selection process of practitioners and also during the ongoing evaluation of the practitioners already employed.

Bearing in mind the Simon and Levin experiment it becomes easier to highlight the discrepancy in the video of the Al-Baghdadi, ISIS leader, 2014 proclamation. In fact, even though the analyses seem to have missed this,

analysing the video it becomes clear that it is a collage of numerous frames. As Al-Baghdadi is climbing the stairs, everybody focuses on his facial expression while ignoring how the lights in the video are switched on and, a second after, are switched off. This discrepancy highlights that the video has been shot several times and only after, in the post-production, has been put together for the audience.

Watching the video now, aware of how change blindness affects everyone, it is easier to detect the discrepancy, however an intelligence practitioner or an analyst affected by change blindness could have missed those discrepancies making a wrongful analysis. The World Health Organization says that the 75 per cent of the population suffers from slight change blindness and that the other 25 per cent suffers from severe change blindness.

What is scientifically defined as Unilateral Spatial Neglect (ICD-10-CM 2018) can be categorised in this type of bias as well, physiological bias. Categorising the Unilateral Spatial Neglect as a physiological bias enables to start working and find solutions. The Unilateral Spatial Neglect is a spatial cognition disturbance that affects people that have suffered from cerebral traumas or incidents, individuals pathologically conditioned or sane people who are highly stressed and/or conditioned by external situations such as family, society etc.

To make it clearer, it is something that might happens to a policeman while driving his car during a chase. Due to the stressful situation, his sight will thin into a tunnel (allowing him to see only the car he is chasing excluding the rest).

The Unilateral Spatial Neglect modifies one's thinking, the stress makes the individual unable to have a correct and objective vision of what surrounds him. It is important to notice that the term 'correct' has been used on purpose instead of 'real' as reality could be different for every individual.

Thanks to numerous studies it has been highlighted that the Unilateral Spatial Neglect, which can be left or right sided, affects at least the 30 per cent of the population. In other words, eyes are slaves of the attentive system, therefore, one's elaboration process interferes in everything anyone reads or sees. Thus, the power of that elaboration process is the base of how individuals perceive anything they see. The more one sees the more one's brain creates his own elaboration of reality.

Cases have been studied in which individuals describe things that in reality were not there, or would report particulars incoherent with what they see, as it happens with individuals affected by Unilateral Spatial neglect syndrome. These subjects' brains perceive only a portion of the image they

have seen and then replicate, in an identical way, that portion to cover what is missing of the image. For instance, their brain would see only half of someone's face and would replicate that half twice in order for the individual to have the image of the entire face. Although, in doing so, they could miss the scar on one side of the face, for instance, or replace a missing eye.

For the intelligence practitioner and the analyst it means to collect and/or provide wrongful information, his biases, his perceptions, create a reality that is not the correct one. These concepts are very important also for the experts that create algorithms and technical instruments for the intelligence work, because if the machine is created and programmed by a human being with biases, the machine will have the same biases, the same failures.

Even in regard of Artificial Intelligence there would be artificial brains analysing with biases; this unveils a new study and evolutionary scenarios linked to cyber-sciences. At today, given what it is known, everything that has been created relating to Artificial Intelligence is flawed by the very fact that whomever has created the machine has unintentionally inserted his own parameters and biased perception/views.

Hence, using an Artificial Intelligence to perform intelligence analysis or any other task/operation is limited by the fact that the Artificial Intelligence does not have a correct initial building structure. If the human being has biases caused by the society, he would program a machine with his own limitations and biases.

Yet, even the analysis of an unbiased machine cannot be completed without the human intervention, because the human being is always able to update scenarios and strategies while the machine cannot, and to correlate the information the machine provides. The machine error is caused by the variables that the human being introduces, the more unbiased is the human being the better information the machine will provide.

As the programmers are technicians, they develop programs based on the information given by the intelligence, if the operator has a biased perception that does not see as dangerous a seventeen years old Turkish-German boy the machine won't signal the individual as dangerous because he does not fit the set parameters (as it happens in Monaco in 2015)

That is why is extremely important to eliminate the operator's biases. Eliminating the operator's limitations of thinking enlarges the range of connections the machine will be able to analyse and increases the possibilities to detect threats. It is possible to train an operator to be able to develop programs for a machine that can provide good results.

What seems to be scientifically so difficult is nothing more than a return to simplicity and humbleness, in order to understand the world for

what it really is and not for what individuals think it to be. For the intelligence to be effective and based on the real scenario, it is necessary to give to words and events their correct value, to return to the real meaning of words that are the instruments through which everyone communicates, expresses idea, gathers information, makes analysis.

Lately, the discourses regarding the Islamic religious terrorism that have attacked Europe in the recent years have been focused on the term radicalisation, committing a huge mistake.

What the word radicalisation really means?

If I talk with a theologist it means a process that takes up to eight years before its conclusion, in fact a boy that would want to become a priest would have to go through an eight years long path before becoming one; while if I talk with a psychiatrist – the word radicalisation – indicates a process that takes at least seven years, the time a psychiatrist would need in order to definitively reprogramming the brain of a worshipper of a cult.

Its scientifically impossible to define as "radicalised" a subject that becomes interested and get close to religion, practising all dogmas, in a couple of months. The cognitive process -that allows to encode the information- needs time in order to permit the writing of neural cells in the brain (for instance, choosing to start the elementary school at five/six years it is not a random choice as at this age the areas of the child's brain are formed and ready to learn).

Numerous studies have proven that for a radicalised individual to actually change his/her behaviour and mind-set requires not less than seven-eight years, so that s/he can interiorise contents, ways of thinking and elaborations. However, lately the word radicalisation has been used to indicate terrorists that, from the information gathered, got close to that pseudo-religion only few months before the attack.

It is easy to understand how one of the major mistakes of the intelligence analysis has been to define radicalised individuals that could not be radicalised, and in doing so, let those individuals that have committed the recent attacks in Europe pass unobserved to the analysis.

Simplifying, if the intelligence practitioner would ask a technician to develop a program aimed at looking for radicalised individuals, the latter would use the scientific radicalisation parameters. He would complete the task he has been given but developing a program with a high margin of error in searching for the today`s terrorists who, as it has been explained, cannot be

defined as radicalised. A communication error at the base leads to the creation of wrongful models.

Yet, it could have been possible to improve the algorithms and provide results if theological and psychiatric concepts, as the one of 'infatuated' (École Universitaire Internationale research centre, 2017), would have been taken into consideration, that would have allowed to specifically detect individuals as those who committed the attacks. The machine looks for what the human being programmed it for, if it has wrong parameters it will provide wrongful results. If the goal is to detect this type of terrorists, the analyst must look for infatuated individuals with all necessary medical, sociological, psychological parameters that characterised them. Yet, words must have a unique meaning (unless they are thought to be intentionally misleading like psychological-operations can do).

Moving back to the word radicalisation: If the analysis is made by someone that use theological or psychiatric concepts we will obtain a result; if the analysis is made by someone that use the common concept of radicalisation that everybody talk about we will have an opposite result. Taking this into account, it is easy to understand how this error at the foundation of the analysis causes repetitive errors that, like a waterfall, lead to a wrongful analysis and results.

Scientifically we cannot define radicalised any of the individuals that have committed the recent terrorists attacks in Europe in the last years. Nor we can use the word 'quick radicalisation'. Radicalisation, in its true meaning, cannot be a quick process.

These terms induce in error who makes the research and who makes the investigation in the field of the today Islamic terrorism. These individual can be defined as "infatuated" rather than radicalized. They have different characteristics from those that a real radicalised individual would have, therefore also the security algorithms used to identify these individuals need to be based on different criteria otherwise they won't be able to early detect and identify the threat.

Thinking of a radicalised individual, we would refer to a grown up man with a long beard that would never blend in the European culture. While if analysing the profile, the 'social profile' of those individuals that have committed the recent terrorist attacks in Europe, who have been defined as 'infatuated', arises characteristics completely different. A radicalised individual would never have a personal social profile, not to confuse with other possible social profiles created by terroristic groups for communication or to look for new worshippers. Social profiles, in fact, are an invention of the 'western Satan', and so they go against the Quran dictates. Yet, every

youth who has committed one of the recent terrorist attacks in Europe had a social profile.

These terrorists are individuals born and raised in Europe that identify themselves as Spanish, French, and German. This comes to light considering what the terrorist in Germany yelled during the attack in 2015 "I am German! I was born here!". This becomes evident looking at their social profiles pictures; they are dressed as any other western guy would, jeans, sneakers, hats and sunglasses (most of which with western recognisable brand).

They are not strong radicalised individuals that hate the western society but rather individuals wick, with a wick connection with both their origins (Arabic Countries) and the state they have been raised into (European Countries). There is also another particular element that comes to light analysing their social profiles' pictures: most of them wear tank tops (Magris, Fanti, 2017), tank tops that are usually worn by body-builders to show their muscles, as if they want to flaunt a masculinity they do not have. Analysing the social profile pictures the terrorists hedonism comes to light, the attack seems to be an attempt to reclaim themselves rather than an ideology.

The tank top is a symbol and appears dissonant with the bodies of these youth. Even their posture is dissonant; they appear to be flaccid, with rickety shoulder, far away from the image of the macho icon. Radicalised individuals wouldn't wear western clothes or western brands nor they would have a social profile. If the analysis would have looked for an infatuated individual it would have been easier to detect individuals like those who have committed the recent terrorist attacks in Europe.

Only reading the Quran would take several months while contemplating its meaning would take several years. Numerous verses have come to Mohammed to respond to specific problems such as in the occasion of battles to face alongside his faithful or to bring peace in community disputes, it is in light of these circumstances that these verses should be read. Uses and customs of those times should be known and taken into consideration in understanding the Quran. Yet, the Quran has many biblical references, therefore it is necessary to also read the entire Bible in order to truly comprehend the Quran. However, that won't be all, as to deeply comprehend it, it would be necessary to read also the Torah. Reading the Quran, the Torah, the Bible, studying Mohammed life and the broader Middle East story are just the first steps to beginning to grasp and understand the Islamic religion.

These youth show a mask they cannot wear linked to the self-external reflection and self-perception. This triggers a strong internal conflict on how the individual perceives himself that increases his frustration. We can see this

also in the way they are looking at the camera: their look is empty, passive, and apathetic and pride less.

Underlining the parameters and characteristics above mentioned it is easier to detect and notice them, however a practitioner with biases would hardly detect them and connect the dots. Yet, it is possible to train an operator to have as fewer biases as possible. First of all, to overcome these biases, the operator should know that biases exist and that they can mislead his/her perception.

S/He should be trained to have a scientific interdisciplinary background. This does not mean that the operator has to know everything about everything but S/He should be able to use different practical tools that derives from different disciplines such as psychology, sociology, neurobiology, neuropsychology, theology and others that are often not considered.

Here is where the evidence-based research filled the gap between academia and intelligence, enabling the operator to use tools that are based on scientific disciplines in the intelligence work.

Researchers by École Universitaire Internationale have proved that in order to reach a successful result, information must be easy to understand for the operator. The trainer must be able to explain those tools without necessarily explain all the science behind, because sometime there is not enough time to explain all concepts. For instance the operator does not need to know how the cortisol is produced within the body, but he or she needs to know that high level of cortisol affects the individual behaviour making him less focused and more irritable for more than 48 hours, and be able to use this to his/her advantage if necessary. The operator has to know the practical applications of information but S/He does not need to have the scientific preparations of all disciplines.

The '*Frullbrain*' method has been ideated and conceived to create education (for both the mass and the individual), it has been tested and applied in the past five years to a sample of about 2000 individuals reaching positive results in the 98 per cent of cases. École Universitaire Internationale researches have shown that training conducted with this method enable the practitioner and the analyst to have a remarkable bias reduction, a brain that permits to analyse the information in a flexible and correct way enabling him/her to detect the true information.

The first results, which consist in developing a different way of analysing the information surrounding the practitioner, are reached after eight hours of the '*Frullbrain*' method application. Again, the method enables who works in the field to be able to understand the scenario in which S/He is involved and to put in practice the best strategies to perform the task. The

training conducted this way, using of neuro-psycho-pedagogical method as the one developed by École Universitaire Internationale, allows any practitioner to perform the job at the best level increasing his/her cerebral and cognitive capabilities of the 35-37 per cent. Techniques tested on aware and unaware individuals (to guarantee the results) based on written protocols, enable to obtain the desired chemical reactions in order to obtain the desired reactions from the operator. For instance, increasing of cortisol, decreasing of adrenaline, managing of i-mao enabling to remotely trigger reactions in an individual or to train the operator to obtain the right reactions based on situational needs.

Conclusion

The narrative of the recent terroristic attacks is a spot narrative. The terrorist grabs the first tool he founds (i.e. a knife) and performs the act yelling *Allah Akbar.* The narrative is short, very short, making really difficult to detect the early initiation signals.

Carrying out an accurate research/identification of individuals using specific parameters is extremely important, as performing a spot act, the only rule they follow is self-advertising, personally posting selfies and videos that serve the goal to self-feeding their ego without even realising they do not have an audience to applaud their deeds.

The narrative can be defined as spot narrative because it is a short story of the event. They did not plan the attack based on alleged Quran indications or dates, they do not know the Quran. These individuals did not read more than five pages of Quran, their acts are merely an emulative attempt in order to feel important based on common stereotypes. Even the pictures in which they held firearms, as guns or *Kalashnikov*, reveals their inability in using firearms, holding them is simply aimed to the self-production of photographic and visual materials.

If this individuals would have had the physical characteristics and the chance, they would want to work for an American movie major, or play football for an important club – they only want to find a place in which express their ego -, showing the complete absence of any real repulsion to the 'western Satan' whatsoever.

They are individuals with no identity, this is why it could be helpful to complement fake news with web sites and structures that offer alternative identification for the mass of youth. This could represent a quick and cheap solution to apply in this kind of activities.

The majority of the terrorists had planned normal social activities for the evening or the day after their spot, showing no understanding of the harmful/negative consequences it would have had for them. They show an acute cognitive bias affecting their perception of the consequences of the act they committed, as if their act was less valuable than a simple video-game match. This said, this does not in any way gives them neither any attenuating circumstances nor any possibility to appeal to any mental disease to reduce their responsibility for the actions they committed.

References:

1. Bellomo, Davide, (April 2018), "What is biased can be unbiased: the neurological process of identification and elimination of biases held by professionals and victims. Study conducting using subject's brain mapping to evaluate biases caused by trauma, culture or education" EVAWI International Conference, Chicago (USA).

2. Bisiach, Edoardo, Luzzatti, Carlo, (1978), *Unilateral neglect of representational space*, Cortex.

3. Bisiach, Edoardo, (2004), *Spatial neglect. A representational disorder?,* Ed. Elsevier Masson.

4. Cambridge Advanced Learner's Dictionary and Thesaurus, (2018), Cambridge University Press.

5. Cummins, R.A., and Nistico, H., (2002), "Maintaining life satisfaction. The role of positive cognitive bias", in Journal of Happiness studies.

6. End Violence against Women International, (2018), International Conference Chicago (USA).

7. Frullbrain Method, (2017), École Universitaire Internationale Rome.

8. Grassi, Martina, (2018), *"Who is the terrorist? Sociological analysis of the "social profiles"* International Association for Intelligence Education (IAFIE), Leicester UK, September.

9. Guariglia, C. et al., (2013), *"Neglecting the left side of a city square but not the left side of its clock: prevalence and characteristics of representational neglect".* PLos One, p. 7.

10. Hendrickson, Noel, (2008), *"Critical Thinking in Intelligence Analysis",* International Journal of Intelligence and CounterIntelligence.

11. Heuer, R.J. Jr., (1999), *Psychology of Intelligence Analysis*. Center for the Study of Intelligence – Central Intelligence Agency.

12. Heuer R.J. Jr., (2015), Pherson R.H*., Structured Analytic Techniques for Intelligence Analysis*, CQ Press, second edition.

13. Iacopino, V., Xenakis, S.N., (2011), *"Neglect of medical evidence of torture in Guantanamo Bay: a case series",* PLoS Med 8(4): e1001027.

14. ICD-10-CM Diagnosis Code H53.9 – 2018.

15. ICD-10-CM R41.4 Neurologic neglect syndrome – 2018.

16. Magris, Sabrina, (September 2018), "*Counterterrorism: new training methods to eliminate biases. Deactivating the terrorist analysing the terrorist's psychological profile"* International Association for Intelligence Education, (IAFIE) Leicester UK.

17. Magris, Sabrina, Fanti, Francesca, (2017), *Terroristi in canottiera. L'universo di significati che si celano dietro un simbolo,* EUIEdizioni Roma.

18. Magris, Sabrina, (2015), *Ossimoro.* Dove ogni cosa può avere mille significati. *Psicologia operativa applicata in ambito di intelligence, terroristico e criminologico,* EUIEdizioni Roma.

19. Marshall, J., Robertson, I., (2013), *Unilateral neglect: clinical and experimental studies*, Lawrence Erlbaum Associates, Publisher. *Brain image, behaviour and cognition series.*

20. Moscovici, Serge, (1976), *Social influence e social change,* Academic press.

21. Nickerson, S., (1998), *"Confirmation Bias: A Ubiquitous Phenomenon in Many Guises"*, *Review of General Psychology*, Vol. 2, No. 2, pp. 175-220.

22. Palermo, L., et al., (2010), *"Does hemineglect affect visual mental imagery? Imagery deficits in representational and perceptual neglect"*, Cogn Neuropsychol 27(2): 155-33.

23. Simons, Daniel, (1999), Chambris Christopher *Experiment "The invisible gorilla"*.

24. Simons, Daniel, Levin, Davis, (1998), Failure to detect changes to people during a real-world interaction, *Psychonomic Bulletin and Review*, 5, pp. 644-649.

25. Winnicott, Donald Woods, (1960), "*Ego distortion in terms of true and false self. The maturational processes and the facilitating environment: study in the theory of emotional development",* Karnac Books, London, pp. 140-152.

CYBER INTELLIGENCE

ESTONIA CYBER-ATTACKS AND THE IMPACT ON NATO

Alexandra Elena TIMOFTE*

Abstract

Out of all the industrial or technological revolutions that ever occurred throughout the history the latest one marked all the components of human life. But development comes with diversification of vulnerabilities and threats. Thus, the providers of security are forced to have the proper response facing all kind of threats, conventional and non-conventional (hybrid threats) starting with the military dimension to the digital or cyber space.

9/11 and the cyber-attack against Estonia were both conducted through non-conventional means, they were both affecting the civil population and not only the government or the politicians, both were aiming to weaken the national security of the countries targeted. But what impact did these two events have on NATO? How was each perceived at the level of the Alliance and what was their outcome? A terrorist attack is producing way much greater impact upon the public compared to a cyber-attack which can hardly cause such major visual effect. However, the latter, in the context of the fast digitalization of the present days, can seriously damage the government services and decrease peoples trust. In this realm a real and comprehensive response to the new threats is required, not only from the states as sovereign entities but also from the organization at the international level.

Keywords: *cyber-attack, cyber defense, non-conventional means, non-conventional threat, terrorist attack.*

Introduction

A terrorist attack caused by crashing a plane into a building is having way much greater impact upon the public compared to a cyber-attack which can hardly cause a major visual impact. However, the latter, in the context of the fast digitalization of the present days, can seriously damage the government services and decrease people's trust (Ciolan, 2014).

* National School of Political Studies and Public Administration, timofte.alexandra26@gmail.com.

On this realm a real and comprehensive response to the new threats is required, not only from the states as sovereign entities but also from the organizations at the international level. The subject of this paper is the cyberspace (especially the cyber defense) analyzed from the perspective of one of the most influential military Alliances still existing nowadays: NATO. The reason why I choose this topic is due to its growing importance, but most of all, due to the events that occurred within this domain: the cyber-attack on Estonia in 2007. These events generated important discussions regarding the behavior of the actors in the cyber space and the level of jurisdiction that can be applied to this domain.

The questions of the following research are: Why in the American case Article 5 was triggered and in the Estonian case not? What were the consequences of these two events on NATO, especially after the 2007 cyber-attack? The method I will apply will be comparison. I chose to compare the impact that the 9/11 terrorist attacks had on the Alliance (that moment being the first and the only one when the Article 5 of the Alliance was invoked) with the events from Estonia, which did not trigger the Article 5 of the Alliance. Nevertheless, as it will be shown, the latter event brought cyber-security problems on the diplomatic agendas of NATO officials, generating important changes within the organizational framework and on the political perspective of the cyber space.

I choose to compare the two events due to the different impact they had despite the similarities between them. As I will illustrate in the following pages, 9/11 and the cyber-attack against Estonia were both conducted through non-conventional means, they both affected the civil population and not only the government or politicians, both were aiming to weaken the national security of the countries targeted. After this process I will analyze the impact on NATO and the actions taken by the Alliance. At this level I will illustrate the main differences reflected not in the manner that were conducted, but in the way they were perceived at the level of the Alliance: in the first case we have a clear response, a day after the attack, while in the second case we have no immediate response, but a step by step approach focused on defensive measures.

The paper is structured in four parts. The first chapter will introduce the concepts of non-traditional threats and non-traditional actors and the emergence of these two during the 21st century as part of a larger subject – the hybrid war. The second chapter will present the two selected cases in which the concept of non-traditional threats is exemplified: the terrorist attack on 9/11 and the cyber-attack on Estonia conducted in April 2007. In the third chapter I will compare the two cases, and I will identify differences and

similarities from a NATO perspective and will emphasize the main actions undertaken by NATO as a possible response to the cyber-attack on Estonia. The last of the paper will be reserved for a series of final remarks.

The emergence of non-conventional threats on the international arena

During the last decades, the security field suffered some changes, being widened both horizontally (including more domains) and vertically (including different kind of actors). Horizontally, besides the political and the military fields, economic, cultural and environmental ones were added (Buzan, 2014). While in terms of actors, the limitation to the state was overcome by the introduction of the individual. However, at the international level a wide variety of actors exist, from states and individuals, to different types of organizations and groups of individuals. But the widening concept of the security field meant a variety of the possible threats. Specifically, the diversification of the nature of the actors present on the international arena and the possible threats and challenges posed by them in the 21st century gave birth to a new category of threats: the so called non-traditional ones. For example, in a 2014 article published in the *International Journal of Development and Conflict* it is argued that "rise of non-state actors, intra-state wars, environmental degradation and climate change, demographical changes and cyber-conflict pose a greater security threat to the nation-states in the 21st century than armies of other states." (Srikanth, 2014)

The non-traditional threats are the opposite of the idea of solely conventional threats seen especially as organized military components. The hybrid threats are included in this category. The causes of emergence of these threats are various: from globalization, to technological revolution and the spread of democracy. My main focus is to see which are these new threats and their impact, with a special focus on NATO. The definitions of these new types of threats vary from one author to another. For example, from the perspective of a military practitioner the hybrid threats are represented by the actions of an opponent that "simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism and criminal behavior in the battle space to obtain their political objectives." (Hoffman, 2009)

Other see the hybrid actions as including also cyber offensive and psychological operations (Hunter, Pernik, 2015). Figure 1 – Hybrid threats (Purton, 2015) depicts the hybrid threats as representing the core of a combination of actions such as conventional, irregular and criminal means, but also acts of terrorism.

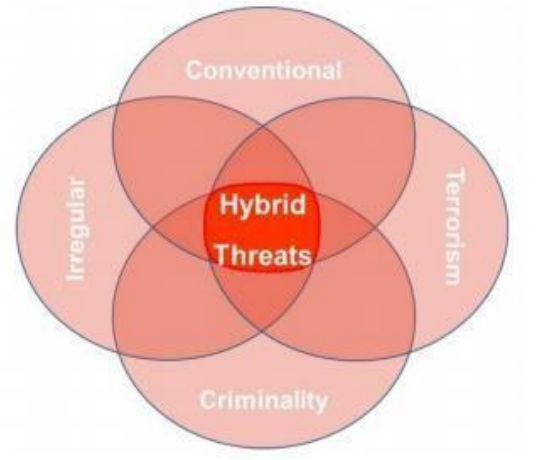


Fig. 1 Hybrid threats

An even more comprehensive view of what the hybrid threats is provided by NATO: "multimodal, low intensity, kinetic and non-kinetic threats to international peace and security including cyber war, low intensity asymmetric conflict scenarios, global terrorism, piracy, transnational organized crime" (Richterová, 2015).



Fig. 2: Hybrid threats – NATO perspective

Not only the action *per se* has been analyzed, but also the actors involved. The importance of the actors in the case of hybrid war is essential for understanding this type of threats. At the international level we have two main categories of actors: state and non-state actors. If in the first case the understanding is clear, in the second case things are more complicated. In the category of non-state actors, just as the term is saying, the actors that do not speak in the name of the state are included. The problem arises from the multiplicity of non-state actors that can be represented either by organizations (international relations), corporations (international economic relations) or by individuals or groups of individuals. At the same time, at the international level we encounter official and unofficial positions of states regarding the problems present. For example, even though some non-state actors, such as terrorist organizations or hackers, are declaring they are acting on their own behalf, in some cases they are supported and/or sponsored by state actors. In both cases – actions conducted by terrorists or hackers – the link between states and these non-state actors is very fragile and very difficult to be tracked down. The blurred line between the two is making the process difficult. However, the two types of actors are more often included in the non-state category.

From a security perspective, the most important problem is when a non-state actor is challenging the legitimacy of a state actor by using violent means. The challenges posed by the non-state are not necessary new, but in the 21st century this phenomenon gained more and more attention because we are witnessing a particular mixture between the non-state actors and the new technological tools. Due to this last component, weak non-state actors (such as individuals or group of individuals) are posing a real threat to the security of a state. Even though the power of a state in terms of military means is greater than the power of any individual or group of individuals, the use of irregular and nonconventional tactics by the latter, in some cases, overcome the damages they can produce to the former. However, the irregular or non-conventional tactics in order to defeat the opponent are not used only by non-state actors. Historically, even states appealed to these tactics as source of power in order to defeat a stronger combatant. According to this perspective, it can be argued that the hybrid war is the instrument of the weaker part in combat with a stronger force. At the same time, some specialists assert that the hybrid war may be seen, in the near future, as "a smart and nimble tactic." (Hoffman, 2009, p. 34)

These new types of threats have drawn the attention of the North-Atlantic Organization as well. However, compared with United States, the Alliance had a belated response. For example the United States mentioned

the term hybrid threats since the first decade of this century, while in the NATO documents we encounter this especially starting with 2010. Even if in the 2010 NATO *Strategic Concept*, the word hybrid is never mentioned, there are clear specifications regarding the security challenges existing at the international level. Besides the acknowledgement that "the Euro-Atlantic area is at peace and the threat of a conventional attack against NATO territory is very low" (NATO, Strategic Concept, 2010, p. 3) the 2010 *Strategic Concept* expresses a clear concern regarding the "new threats": proliferation of chemical and biological weapons, missiles, terrorism, modern technology in the hands of terrorists, illegal arms trafficking, narcotics and people, cyber-attacks (NATO, Strategic Concept, 2010, p. 3). Apart from the graphic pictured above, within the Alliance, the hybrid threats are defined as "those posed by adversaries, with the ability to simultaneously employ conventional and non- conventional means adaptively in pursuit of their objectives." (Bi-Sic Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats", 2010, p. 2) The definition accepted by NATO resembles to some extent the one given by Hoffman. What is important though: none of the definitions is pointing to a specific category of actors. They can both encompass state and non-state actors which can use a mix between conventional and non-conventional means in combat. Moreover, in the NATO chart, the inclusion of both terrorism and cyber-attacks on the non-kinetic category can be noticed. I am making this observation because it is of vital importance for understanding the following part of this paper which includes case studies for two important events: the 9/11 terrorist attacks on USA and the cyber-attacks on Estonia in April 2007.

The non-conventional aspects of the 9/11 and April 2007 attacks and their impact on NATO

The beginning of this century has been marked by one of the most terrifying events in the recent history: the terrorist attacks on 11th of September 2001. Four commercial planes were hijacked by 19 individuals. Two of the planes were crashed into the symbolic buildings of US power: The World Trade Center; another one hit the headquarters of the US Department of Defense, the Pentagon; the fourth plane crashed somewhere in Pennsylvania, not reaching its target (BBC, The 9/11 terrorist attacks). The entire operation was claimed by Al-Qaeda, a terrorist organization located in Afghanistan. The impact of this event was huge. With almost 9000 casualties (Plumer, 2013), 3000 dead and 6000 wounded, the 9/11 attacks represent a turning point in history. The US president at that time, George W. Bush,

labeled the events as "evil, despicable acts of terror" (BBC, The 9/11 terrorist attacks) and stressed that United States is facing a new and different kind of enemy (*The 9/11 Commission Report*, p. 330).

Six years after this event, another important incident occurred: the cyber-attack against Estonia. At the end of April and beginning of May 2007, Estonia was the target of one of the most powerful cyber-attacks in history. Since the technological revolution at the end of the XX century, other cyber-attacks were conducted, but the one against Estonia had some particularities due to the features of the targeted country. Estonia is one of the most wired countries on the Earth. The range of activities done by internet is widespread and it includes sectors as: e-government, e-voting, e-taxes, e-parking, e-banking, e-identification systems. That is why Estonia is a country that admits the access to internet as being part of the basic human rights (almost the entire country is covered by free Wi-Fi networks) (Laasme, 2011, pp. 58-63). The wide coverage of the Internet and the use of it in almost every daily activity comes with major responsibilities for the state, measured in terms of the capacity to secure the networks and to prevented the collapse. In this sense, the digital space is becoming a part of the national security. Thus, when, in April 2007 a near-catastrophic botnet hit almost the entire electronic infrastructure of Estonia, the national security of this state was threatened. (Laasme, 2011, p. 60) The relevance of this incident is highlighted by the fact that, never before, an entire country happened to be a digital target. (Laasme, 2011, p. 60)

As it can be noticed, both cases, the 9/11 and the events from 2007 that occurred in Estonia can be included in the category of non-traditional threats. In the first case we encounter the use of non-military means (theft of passenger aircrafts crushed into targets strategically chosen) in order to affect and challenge the security of a state. In the second case, we also have a new type of threat, distinct from the conventional, military one: cyber-means used in order to affect the security of an entire state in terms of electronic infrastructure. From a NATO perspective both events have had impact on the Alliance. In the following pages I will summarize the most important measures undertaken by NATO, first, after the terrorist attacks on 9/11 and second, after the April 2007 cyber-attack. Both cases will be analyzed only from the perspective of non-traditional threats.

In the case of 9/11, the answer from NATO was out of hand. In less than 24 hours the Secretary General of the Alliance at that time, Lord Robertson notified the UN Secretary General about the decision made by NATO member states: to invoke the principle of Article 5 from the Washington Treaty (NATO, "Collective defense – Article 5"). This was the first and the

single time in the history of the Alliance when the principle of collective defense was invoked. Even though it was not an armed attack in term of means, the major consequences of these actions lead to a firm and immediate response from the Alliance. In October 2001 NATO agreed on eight measures proposed by US that were tackling: the intelligence information sharing, the support to the countries that are subject or possible subject of any terrorist attack as a result of their involvement in combating this phenomenon, increased security on their territory to any facility provided by the allies, the access to any ally to their ports and airfields for operations against terrorism, the deployment of the Alliance Standing Naval Forces to the Eastern Mediterranean, the readiness of the Alliance to deploy part of its Airborne Early Warning Force in order to combat terrorism (NATO, "Collective defense – Article 5"). Starting the same month operation *Eagle Assist* was launched – the first anti-terror operation, consisting of patrols over the sky of United States.

One of the most important actions of the Alliance was the empowerment of NATO to take the lead of the International Security Assistance Force (ISAF) mission in August 2003. Due to the fact that Al-Qaeda was localized mainly in Afghanistan, the international coalition transformed this country in the main target of the anti-terrorist actions. The aim of the ISAF mission was to help the Afghan government to provide security to the country and in the same time to ensure that Afghanistan will never become a *safe-haven* for the terrorists (NATO, ISAF mission in Afghanistan (2001-2014)).

In the case of Estonian cyber-attacks we have a different range of actions and measures taken by the Alliance. Even though the attack affected the national security of Estonia, the way in which the attack occurred did not represent a case to trigger the Article 5. In 2008, in the declaration of the summit held in Bucharest was stated for the first time the need to strengthen the key Alliance information system against cyber-attacks (NATO, "Bucharest Summit Declaration", 2008).

Furthermore, in the strategic concept issued in 2010 the fact that the cyber-attacks are more and more frequent and the impact of such attacks on the government administration, business and critical infrastructure of the Allies can be very disruptive is highlighted (NATO, Strategic Concept For the Defense and Security of the Members of The North Atlantic Treaty Organization, 2010, p. 3). In response to these threats, in the same document the need of a centralized protection of the Alliance and enhanced coordination of cyber-capabilities of the member states was specified (NATO, Strategic Concept For the Defense and Security of the Members of The North Atlantic

Treaty Organization, 2010, p. 3). Beside these measures, maybe the most important one is the decision of the Alliance to "recognize cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea" taken at the Warsaw summit held in July 2016 (NATO, "Warsaw Summit Communique", 2016). At the operational level, the Alliance's preoccupation for the cyber-space started in 2002 when the NATO Computer Incident Response Capability (NCIRC) was initiated[1], but which was fully operational in 2008. The same year the Allies ratified NATO Cyber Defense Policy and decided to create the Cyber Defense Management Authority in Brussels. In May 2008, the Cooperative Cyber Defense (CCD) Center of Excellence (COE) was established in Tallinn (NATO opens new center of excellence on cyber defense, 2008). CCD COE aim is to give support to its member states and NATO members in the fields of technology, law, strategy and operation (CCD COE, "About Cyber Defense Center"), but it does not belong to the NATO military command or force structure (CCD COE, "About Cyber Defense Center"). It is widely accepted that all these measures were hasted by the events that occurred in Estonia in 2007.

Comparison: similarities – differences

If the previous chapter I presented the main aspects of the two events I chose to compare. In the second part I described the impact that the events had for NATO and the direction the Alliance choose after both of them. The following comparison will be in regard only the two cases from the perspective of NATO and the perceived non-traditional threats.

On the one hand we have the 9/11 terrorist attack which triggered the Article 5 of the North-Atlantic Treaty. The attack was conducted by the terrorist organization Al-Qaeda by appealing to nonconventional means: they transformed three passenger aircrafts into weapons, hitting strategic targets inside United States, causing a great number of casualties. On the other hand, we have the use of cyber-instruments as non-conventional means targeting the entire electronic network of a country. Estonia's electronic infrastructure was struck by almost one million computers at the same time, attack which was coming from hijacked computers from United States by unknown elements inside Russia. (Laasme, 2015, p. 60) In this case, even the Estonian officials linked the attack with the decision to remove a Russian statue which

[1] It is the main instrument developed by NATO in order to protect the networks of the Alliance. It includes Rapid Reaction Teams which are designed to help the member states in protection of the networks.

was commemorating the Russian victims from WWII. At the level of NATO there was no declaration that the Russian Federation is behind this attack.

Until this moment we can identify a series of similarities. First, both actions are included on the list of non-conventional means that can be used by any adversary in a combat. There has not been used any military infrastructure in order to undermine the national security of the two countries. Second, the nature of the actors: in the 9/11 case we have a group of individuals labeled as terrorist organization (non-state actor), in April-May 2007 attack we do not have a clear identification of the attacker. In this case, even if we do not know who conducted the attack, at least the possibility to be a state actor was not fully acknowledged. Of course, the second similarity is having some weaknesses due to the fact that the actor involved was not identified at all.

Nevertheless, it is important that NATO did not rush in linking the attack to Russia. As I mentioned above, the terrorist organizations or the hackers can be supported or controlled by states, but in the cases in which the link between them cannot be demonstrated, hackers are remaining non-state actors.

A third similarity is the target of the attacker. In the case of 9/11 the terrorists hit civilian buildings and caused casualties among civilians in a deliberate way. The Pentagon was also hit, a building of the government, but this cannot be considered part of the military or combatant in a conventional war. In the Estonian case, due to its widespread use of digital space, also the civil population was highly affected because, as I mentioned above, Estonia is using: e-government, e-banking, e-identification system and the list continues. Even though the Estonian government was also the target, the attack paralyzed the entire country which was forced to cut down all the ties with the outside networks, thus affecting not only a limited number of people such as politicians or any other group, but the daily activity of the civilians.

On the other hand, in terms of differences, we can identify some important ones from NATO perspective. The consequences that the events of 9/11 had (9000 casualties), compared to the cyber-attack which caused no deadly victims, but affected the electronic infrastructure of a country. This is a difference at a general level, but at the level of the Alliance the fact that in 2001 NATO chose to take military action and in 2007 not, the difference can be tracked down in the documents of the Alliance. For example, in the Strategic Concept of 1999 was clearly stated:

> *Any armed attack on the territory of the Allies, from whatever direction would be covered by Article 5 and 6 of the Washington Treaty. However the Alliance must take into*

> *consideration the global context. Alliance security interest can be affected by other risks of a wider nature, including acts of terrorism, sabotage, organized crime, and by other disruptions of flows of vital resources.* (NATO, "The Alliance's Strategic Concept")

These specifications from the Strategic Concept from 1999 were an argument in favor of triggering the Article 5 in the case of 9/11. More exactly, in the press release from 12th of September 2001, NATO member states "condemned terrorism as a serious threat to peace and stability and reaffirmed their determination to combat it in accordance with their commitments to one another, their international commitments and national legislation." (NATO, "Statement by the North Atlantic Council")

Thus, in terms of legal framework, the Alliance was entitled to consider 9/11 actions as covered by the principle of collective defense stated in the Washington Treaty.

Another difference is that the events that occurred in Estonia triggered no military actions. Here we can identify the most important difference between the two events from NATO perspective. While the 9/11 event was covered by legal framework, the Estonian case was not. Every decision related with the cyber-space in terms of legal framework was taken post factum. In other words, if there were any specifications in the official documents of the Alliance tackling the issue of cyberspace/cyber-attacks the attitude of the Allies towards this kind of threats, other kind of actions would have been taken. But in this case, only years after, when the member states became aware of the damages that can be produced through cyber means, agreed to include the cyber space on the list of other three (land, sea, air) covered by the collective defense principle.

NATO after 2007: strategy, means and policies

The Article 5 from the Washington Treaty specifies "the Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all" and all the necessary means, "including the use of armed force." (NATO, "The North Atlantic Treaty (1949)")

To consider cyber-space as part of the collective defense principle means that to a cyber-attack even an armed attack as a response is possible. This specific issue brought the attention of the parties involved. That is why one of the most important issues that NATO is struggling to establish is a threshold: to what extents a cyber-attack will be considered as requiring a

military response? In this regard, at the invitation of NATO Cooperative Cyber Defense Center of Excellence a group of international law experts elaborated the Tallinn Manuals which are trying to set these thresholds and the way in which international law can be applied to cyber-space.

Another important issue that is discussed within NATO is the identification of the attacker. Cyberspace is very attractive due to the fact that the user can choose to remain anonymous. To track down the source of an attack in cyberspace is very difficult, thus responded it is very unlikely.

In this regard, NATO strategy for cyber defense is focusing on "the resilience of NATO's and Allies' Communication and Information System (CIS)." (Ducaru, 2016, p. 20) To this strategy is contributing the NATO Computer Incident Response Capability and the affiliated cyber defense Rapid Reaction Teams. In strong relation with increased resilience of the Alliance and its members is the awareness and early warning policy endorsed by NATO, but also the cooperation and exchange of information between the Allies. For the cooperation part we encounter the agreement between NATO's Cyber Defense Management Board (CDMB) and the national cyber defense authorities, while in the case of early warning NATO developed the Cyber Threat Assessment Cell (CTAC). (Ducaru, 2016, p. 19.) In its efforts to secure the cyberspace NATO also developed important instruments of cooperation with other organizations such as: United Nations, Council of Europe, Organization for Security and Cooperation on Europe. One of the most relevant steps towards this aim was made in 2016 when NATO and EU signed a Technical Arrangement on Cooperation in the Cyber Domain. "This Technical Arrangement provides a framework for exchanging information and the sharing of best practices between emergency response teams." (NATO, "NATO Cyber Defense", p. 2)

Conclusions

At the beginning of this paper I proposed to answer two questions:

1. Why in the American case the Article 5 was triggered and in the Estonian case not?

2. What were the consequences of these two events on NATO, especially after the 2007 cyber-attack?

The analysis was conducted from the NATO perspective and the impact of non-traditional threats on the Alliance. Applying a comparative method I succeeded to answer both question during my analysis. For the first question I identified the nature of the means involved in the attack, and I concluded that in both cases non-conventional means were used. This was one of the

similarities of the two cases. But the answer to the question *Why in the American case the Article 5 was triggered and in the Estonian case not?* relies on the differences between the 9/11 attack and the cyber-attack upon Estonia. It can be said that for the events of 9/11 the Article 5 was triggered because the legal framework developed until that moment was encompassing a terrorist attack. In the Estonian case, even if the attack affected the entire electronic infrastructure of the country, the Article 5 could not be triggered due to the fact that no specifications were made up until that point in the official documents of the Alliance. Thus, the main argument in applying the collective defense principle was not the nature of the conflict, but the possibility to justify the actions at the level of NATO.

The answer to the second question is closely linked to the answer to the first question. On the one hand, in the 9/11 case there was a clear military action taken by NATO and its involvement in the anti-terrorist missions, both the actors involved and their location being known. On the other hand, the cyber-attack upon Estonia was not followed by such clear and decisive actions, the entire situation being surrounded by uncertainty. Nevertheless, both events had major impact on NATO. In the 9/11 case we have the first NATO out-of-area mission. In the Estonian case we witnessed a totally different approach of the cyberspace and the cyber defense, the main change being the inclusion of the cyberspace on the list of those which has to be defended alongside sea, land and air.

The 9/11 events can be viewed as a turning point in the policy of NATO if we take into consideration the actions that followed and the declared position of NATO in fighting terrorism. At the same time, the cyber-attack against Estonia is a turning point in the policies of NATO regarding the digital space. The fact that until 2007 very little progress was made at the level of the Alliance in order to tackle the cyber issue, and after the events of the year major changes have occurred, represents an argument in the sense that the cyber-attacks upon Estonia generated the entire flow of improvements at the NATO level.

References:

1. "Bi-sic input to a new NATO capstone concept for the military contribution to countering hybrid threats," 2010, accessible on-line on http://www.act.nato.int/the-countering-hybrid-threats-concept-development-experiment

2. CCD COE, "About Cyber Defense Center", accessible on-line on https://ccdcoe.org/aboutus.html.

3. NATO, „NATO Cyber Defense", accessible on-line on http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet- cyberdefence-eng.pdf.

4. NATO, "The North Atlantic Treaty (1949)", accessible on-line on http://www.nato.int/nato_static/assets/pdf/stock_publications/20120822_nato_treaty_en_light_20 09.pdf.

5. NATO, "The Alliance's Strategic Concept", accessible on-line on http://www.nato.int/cps/on/natohq/official_texts_27433.htm.

6. NATO, "Statement by the North Atlantic Council", accessible on-line on http://www.nato.int/docu/pr/2001/p01- 124e.htm.

7. NATO, "NATO opens new center of excellence on cyber defense", 2008, accessible on-line on http://www.nato.int/docu/update/2008/05-may/e0514a.html

8. NATO, "Warsaw Summit Communique", 2016, accessible on-line on http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

9. NATO, "Strategic Concept for the Defense and Security of the Members of The North Atlantic Treaty Organization", 2010, accessible on-line on http://www.nato.int/lisbon2010/strategic-concept-2010- eng.pdf.

10. NATO, "Bucharest Summit Declaration", 2008, accessible on-line on http://www.nato.int/cps/in/natohq/official_texts_8443.htm.

11. NATO, "ISAF mission in Afghanistan (2001-2014)", accessible on-line on http://www.nato.int/cps/eu/natohq/topics_69366.htm.

12. NATO, "Collective defense – Article 5" accessible on-line on http://www.nato.int/cps/cn/natohq/topics_110496.htm#.

13. "The 9/11 terrorist attacks", accessible on-line on http://www.bbc.co.uk/history/events/the_september_11th_terrorist_attacks

14. "Wartime", *The 9/11 Commission Report*, p. 330, accessible on-line on https://911commission.gov/report/911Report.pdf.

15. Buzan, Barry, (2014), *People, states and fear*, Cartier, Chișinău.

16. Ciolan, Ionela, "Defining cyber security as the security issue of the twenty first century. A constructivist approach" in The Public Administration and Social Policies Review, Vol. VI, 1(12), 2014, accessible on-line on http://revad.uvvg.ro/files/nr12/8.Ionela_Ciolan.pdf

17. Ducaru, Sorin, (2016), „The Cyber Dimension of Modern Hybrid Warfare and its Relevance for NATO", in *Europolity – Continuity and Change in European Governance*, Vol. 10, No. 1.

18. Hoffman, G. Frank, (2009), „Hybrid warfare and challenges", JFQ, Issue 52, 1st quarter.

19. Hoffman, G. Frank, „Hybrid vs compound war", (October 2009*), Armed Forces Journal – Military Strategy, Global Defense Strategy*.

20. Hunter Eve, Pernik, Piret, (2015), "Military Balance 2015, International Institute of Strategic Studies", in *Challenges of Hybrid Warfare*, *International Center for Defense and Security*.

21. Jitka Richterová, (2015), *NATO – Hybrid threats*, Prague, accessible on-line on https://www.amo.cz/wp- content/uploads/2016/01/PSS-Hybrid-Threats-NATO.pdf

22. Laasame, Häly, (2011), "Estonia: Cyber Window into the Future of NATO", *Joint Forces Quarterly*, Issue 63, 4th Quarter, pp. 58-63.

23. Plumer, Brad, (2013), "Nine facts about terrorism in the United States since 9/11", *Huffingtn Post*, accessible on-line on https://www.washingtonpost.com/news/wonk/wp/2013/09/11/nine-facts-about-terrorism-in-911/?utm_term=.ef807ae0f78fhttps://www.washingtonpost.com/news/wonk/wp/2013/09/11/nine-facts-about-terrorism-in-the-united-states-since-911/?utm_term=.ef807ae0f78f

24. Purton, Simon, (2015), "Future Capabilities, Research and Technology, Allied Command Transformation, NATO: "Why half of winning an Irregular War is agreeing on what it is…" in *Background Raport* – "NATO hybrid threats", Prague, accessible on-line on https://www.amo.cz/wp- content/uploads/2016/01/PSS-Hybrid-Threats-NATO.pdf

TO BE OR NOT TO BE RADICAL. FROM ONLINE DISCURSIVE AGGRESSIVENESS TO OFFLINE AGGRESSION

Andrei VLĂDESCU*

Abstract

The exponential development of virtual collective communication favours not only the personal development of individuals but also new ways of expressing negative feelings and thoughts stimulated by the possibility of anonymity and real time dissemination of the opinions. Actually any field of the social life can be reached by the phenomenon of discursive aggression and online harassment, as well as by the launching of rumours or expressing unfavourable opinions towards an individual, a social group (regardless of the catalyst that underpinned its creation – ethnicity , religious, professional or other) or a community.

The new form of harassment, called cyberbullying, can reach mass dimensions when its support are social platforms that favour the rapid distribution of content, adhesion and rallying to a cause, such as Facebook, Twitter, Instagram or YouTube, and the forms in which carry out include: repeated humiliation of a person; sending obscene messages and offensive content; ridiculing by creating a bogus account or blog containing biased information. From the same perspective, online aggression can have multiple effects, manifested individually or together: diminishing the sense of security; increasing anxiety; changes in mood or behaviour; feeding racial or religious prejudices.

On the other hand, whatever it is called cyberbullying, cyberstalking or hate speech, online aggression can be speculated by entities interested in generating short-term or medium-term social tensions or animosities among supporters of diverging political trends, with direct impact on the occurrence of violent incidents, and in the long term generate a fracture between governors and citizens, or even to a diminished the cohesion of a nation, social disorder and dilution of the rule of law.

Keywords: *discursive aggression, online harassment, cyberbullying, hate speech*.

* PhD student, National University of Political Studies and Public Administration, andreivladescu@yahoo.com.

The advanced technologies: better communication and freelance hate

Developing technologies that enhance communication in the virtual environment has positive effects on the personal development of individuals but also negative effects, by opening the door for new and effective ways of spreading negative feelings and convictions, the spread of which is directly proportional to the possibility of anonymizing authors and the real-time dissemination of their ideas.

A 2015 study by researchers at the University of Minnesota and New York University says that increased access to the Internet may explain a growth in the number of hate crimes. Using a large data set compiled from the Federal Bureau of Investigation, the Federal Communications Commission, the U.S. Census Bureau, and the U.S. Department of Labour, the authors concluded that in countries in which broadband Internet access became available at the beginning of the century, the incidents in which hate played a significant role increased by almost 20%. Extended access to the Internet didn't lead to an increase in the foundation of hate groups acting offline, but may have augmented the efficiency of spreading hate ideology and stimulating like-minded persons to carry out attacks (Chan, Ghose, Seamans, 2016, pp. 381-403).

Online tools enable international propagation of message and ease of access (Weede, 2016) to victims, making it problematic to alleviate or hamper negative experiences among users (Cole, 2016) which spend a substantial amount of time operating in that setting. The function of social media is essential in the advancement of social individuality (Popescu, 2016) and self-representation. The online environment adds an extremely pivotal aspect to spiteful and injurious content, furthering its development into something pernicious. (Keipi et al, 2017)

The increase and expansion of the social media has generated significant opportunities for people to communicate and engage in the virtual world. Social media makes it possible for people who would not have been heard in the past, to express themselves. People have access to a vast amount of information on the Internet. Unfortunately, given that social media provides the ideal instrument for fast, limitless and harmful spread of aggressive discourse, it has acted also as a double-edged weapon (Back et al., 2010) by creating an online platform for people who use hate as a mean to attract wider audience often under the veil of anonymity that allows to discard and bypass control and regulation (Bargh & McKenna, 2004; Blair, 2003; Citron, 2014;

Hodges & Perry, 1999). The Internet therefore provides new opportunities for cyberbullying (Hinduja & Patchin, 2008) and cyber hate (Jaishankar, 2008).

The new form of harassment, called cyberbullying, can reach mass dimensions when it is carried out on social platforms that favour the rapid distribution of content, adhesion and rallying to a cause. These platforms, such as Facebook, Twitter, Instagram or YouTube, allow harassment to be carried out in ways that include: repeated humiliation of a person; sending obscene messages and offensive content; ridiculing by creating a bogus account or blog containing biased information. From the same perspective, online aggression can have multiple effects, manifested individually or together: diminishing the sense of security; increasing anxiety; changes in mood or behaviour; feeding racial or religious prejudices.

According to administrative data collected by Active Watch (a Romanian NGO working on the topic of the freedom of expression), for the years 2014-2015, the NCCD registered 53 petitions concerning hate speech (in the form of the violation of the right to personal dignity, G.O. 137/2000, art.15). The most targeted groups were Roma persons, members of the Hungarian minority, people with disabilities and members of the Jewish community. For the same period, the NCCD registered 19 petitions against hate speech purported by politicians, against the Hungarian and the German minorities. The NCCD also registered 10 petitions against hate speech by journalists, against the Hungarian and the Roma minorities (Romani CRISS, 2016).

The Centre for Monitoring and Combating Anti-Semitism in Romania (MCA Romania) publishes yearly reports on anti-Semitic incidents and speech in Romania. MCA Romania published a report summarising the results of the organisation's activity of monitoring Anti-Semitic incidents between the years 2009 and 2014. For the reporting period, MCA Romania identified 65 websites which are considered the main source of disseminating anti-Semitism and discrimination; out of these, 27 websites are active and frequently updated (Monitoring Report, 2015).

Between the hammer of imagination and the anvil of reality

Even if the aggressive discourse in the Romanian social media has not been translated so far into real life through street conflicts between supporters of various ideological camps, what could happen if supporters and opponents of violent ideas were subjects of carefully orchestrated operations by state or non-state entities, interested in creating in our country an explosive situation, generating instability and social fractures? To find any

answers, we can take an analytical look beyond the Atlantic, and if the information disseminated by the media over the past years is not believable to be credible or will be interpreted as part of an informational war, we can consider that what follows is just an exercise of imagination with roots in the real world.

After the violent riots which took place in Charlottesville, Virginia, from August 11 to 12, 2017 under the aegis of Unite the Right, Facebook and Instagram reacted by pulling down accounts and extremist posts from white supremacists. Among the accounts removed were Awakened Masses, Right Wing Death Squad, Vanguard America, White Nationalist America, Right Winged Knight, Physical Removal and Awakening Red Pill, all of which being known for launching calls filled with racial hate. Moreover, because of the links to hate groups, Facebook removed the "Unite the Right" event page as well as posts linked to an article that attacked Heather Heyer (a woman killed by a car that got into a crowd of counter-protesters), published in The Daily Stormer – an American neo-Nazi, white supremacist, and Holocaust denial commentary and message board website (Wong, 2017).

But what happened in Charlottesville and how was it possible for a discursive aggression to lead to the unremitting achievement and overcoming of the point of no return?

In the Unite the Right rally, also known as the Charlottesville rally or Charlottesville riots, the protesters were members of the far-right and members of the alt-right, white nationalists, neo-Confederates, neo-Nazis, neo-fascists, various militias. The marchers chanted racist and anti-Semitic slogans, carried semi-automatic rifles, swastikas, Nazi symbols, Confederate battle flags and anti-Muslim and anti-Semitic symbols. The event turned to violence after protesters and counter-protesters clashed (amongst counter-protesters was a large number of Charlottesville citizens who wanted to show their rejection of white supremacy ideologies, but also supporters of far-left ideologies, like Antifa), and in the aftermath, in the Charlottesville area, in the present days the rally is referred as A12 or 8/12.

According to media, during 2017, the white supremacists practiced military training and they planned the violence that eventually ensued at the "Unite the Right" rally, utilizing specific websites, chat rooms, and social media platforms. They used "alt-tech" platforms like Gab.ai and Discord, and for disseminate operational details they were increasingly used some encrypted chat rooms and apps such as Signal and Telegram. An important detail is that between June 2017 and the moment of the rally, there were over 35,000 extremist messages on the gaming platform Discord (Hu and Brooks, 2018).

Addicted to Chaos

Last August, republican Representative Tom Garrett told CNN, that in a closed briefing the FBI director asserted that Russian interference efforts played a role in inciting what happened in Charlottesville (Foran, 2018). Even if Tom Garrett didn't go much into details, his statement could be related to a BuzzFeed analysis from October 2017 that concluded that an account entitled @Ten_GOP, frequently nominated by media as a fake Russian Twitter user, "appears to have been one of many influential tweeters for the event".

According to BuzzFeed, fake Russian accounts launched over 6,000 tweets that mention Charlottesville, the big majority targeting the sympathizers to the white supremacists. Among these accounts, the aforenamed *@TEN_GOP* account (which had around 140,000 followers), wrote that they were "Watching America destroy itself.. #Charlottesville" and another media reported prominent fake Russian account, *@Pamela_Moore13*, (with roundabout 70,000 followers) said: "Who invented white nationalism? The Democrats. And black nationalism? Ditto. So don't try & blame this on the GOP #Charlottesville".

While the majority of the Charlottesville-related tweets appear to be trying to reach those on the right or even far-right, a number also were aimed at those Americans that oppose white supremacy. That means Russian efforts didn't aim simply at one ideological segment but they did all the best to reach Americans of all political ideologies.

There is no evidence that Russian accounts were involved in organizing the Charlottesville rallies, or they explicitly embolden the white supremacists to commit violence. As with many other events – such as the 2016 elections – is difficult (if not impossible) to quantify the offline impact of their messages. However, as the thousands of tweets show, Russian accounts had an ardent interest in the violence connected to Charlottesville – and we can say that the potential precedent it already set, especially as it came to play with potential or existing divisions.

Reports emerged in media that @TEN_GOP, a Twitter account purportedly managed by the Tennessee Republican Party, was in fact controlled by a Kremlin-backed company, Internet Research Agency, which operated a vast network of troll accounts. Reports show that @TEN_GOP tweeted Russian propaganda, as well as polarizing political content, but it's difficult to assess the size of its influence since Twitter suspended it August (Warzel, 2017).

A hashtag analysis drafted by multimedia artist Erin Gallagher offers a possible clue at how the troll account worked in the case of Charlottesville.

Based on around 6,000 tweets from before, during, and after the Charlottesville #UniteTheRight protests, the chart shows that @TEN_GOP arose as one of many influential message carriers, even if nothing can be said about WHAT it was tweeting and IF it was clearly in favour of or against the white nationalists (Warzel, 2017).

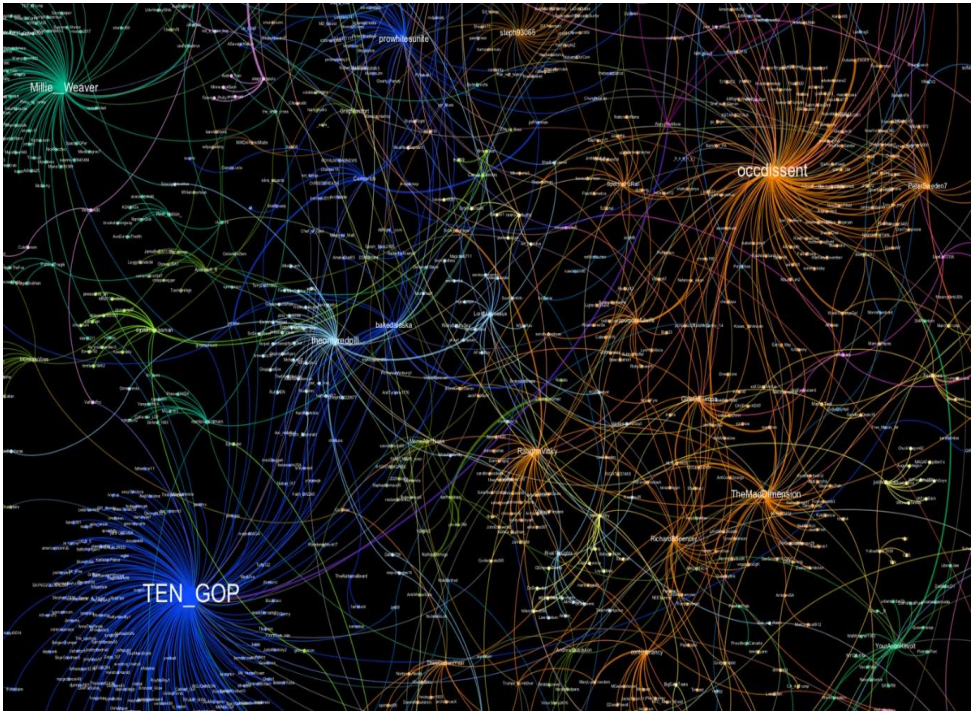


Figure 1 – The position of @TEN_GOP account in the social network created by the Twitter accounts that used the # UniteTheRight hashtag. (Source: www.buzzfeednews.com)

An interesting detail is that #UniteTheRight wasn't the unique case of the @TEN_GOP involvement in something that could something that could have turned into clashes between the partisans of some ideologies and its opponents. Other situations in which media reported the presence of @TEN_GOP were:

- The 2017 Berkeley protests – a series (February 1, March 4, April 15 and 27, August 27, September 14 and 24–27) of protests followed by clashes that occurred in the city of Berkeley, California between organized groups of anti-Trump protesters (including socialists, anarchists, antifa groups) and pro-Trump groups.

- The "March Against Sharia" rallies – in June 11, 2017, a civic organisation, ACT For America, organized (in 28 cities from 21 states) a series of rallies to protest against "the threat to U.S. society posed by the set of traditional Muslim practices", namely honour killings oppression of women, female genital mutilation and homophobic violence.

The Matrioska from social media

The important point is that @TEN_GOP is probably part of a tremendous information war waged across Twitter and other segments of the internet. Even if on its own @TEN_GOP has a limited reach, in the big picture it contributes little by little at the creation and expansion of a narrative aimed to political discord and instability.

On February 16, 2018, the US Justice Department indicted 13 Russian people and 3 Russian companies, accused of conspiracy in order to influence with "US political and electoral processes, including the presidential election of 2016" (Apuzzo and LaFraniere, 2018). The indictment focused especially on the Russian company Internet Research Agency (IRA), whose social media posts and online ads were "primarily intended to communicate derogatory information about Hillary Clinton, to denigrate other candidates such as Ted Cruz and Marco Rubio, and to support Bernie Sanders and then-candidate Donald Trump".

In the indictment, Facebook and Instagram were mentioned 41 times, while Twitter was referred to nine times, YouTube once and the electronic payments company PayPal 11 times (Frenkel and Benner, 2018).

More than that, the document underlined that:

> *"Defendants and their co-conspirators also created and controlled numerous Twitter accounts designed to appear as if U.S. persons or groups controlled them. For example, the ORGANIZATION created and controlled the Twitter account ‹‹Tennessee GOP››, which used the handle @TEN_GOP, falsely claimed to be controlled by a U.S. state political party".*

On May 11, 2018, Democrats on the House Intelligence Committee released the conclusions of an enquiry that revealed the amplitude of IRA activity on Facebook (Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements, 2018):

- 3,393 advertisements purchased (a total 3,519 advertisements total were released after more were identified by the company);

- over 11 million American users exposed;
- over 470 Facebook pages created by IRA;
- 80,000 elements of organic content created by those pages;
- exposure of organic content to more than 126 million Americans.

At the same time, the IRA activity on Twitter in the period between September 1 and November 15, 2016 revealed:

- over 36,000 Russian-linked bot accounts that tweeted about the U.S. election;
- approximately 288 million impressions of Russian bot tweets;
- around 130,00 tweets by accounts linked to the IRA.

As Ranking Member Adam Schiff stated during the Committee's November 2017 open hearing with senior officials from Facebook, Twitter, and Google:

> *"[The Russian] social media campaign was designed to further a broader Kremlin objective: sowing discord in the U.S. by inflaming passions on a range of divisive issues. The Russians did so by weaving together fake accounts, pages, and communities to push politicized content and videos, and to mobilize real Americans to sign online petitions and join rallies and protests.*
> *Russia exploited real vulnerabilities that exist across online platforms and we must identify, expose, and defend ourselves against similar covert influence operations in the future. The companies here today must play a central role as we seek to better protect legitimate political expression, while preventing cyberspace from being misused by our adversaries."*

A comprehensive radiography of Internet Research Agency was published in mid-2015 by The New York Times Magazine (Chen, 2015) and The Telegraph (Parfitt, 2015), revealed some juicy information about the organization. Evoking an ex-IRA employee cited as Ludmila Savchuk, the authors pointed out the intense work at IRA, which is happening during 12-hour shifts (two shifts in a row, followed by two days off), the 400 employees, and the monthly budget evaluated at $400,000. The ex-IRA confessed that IRA had many departments that created content for every well-known social platform: LiveJournal, VKontakte, Facebook, Twitter, Instagram, but also for the comment sections of Russian news outlets.

According to the articles, the employees (most of them around the age of 20) were preoccupied that, after arriving at their job, the main care was to

switch the Internet proxy service, for hiding their IP addresses; over the two shifts they had to accomplish a quota of 5 of the political category, 10 non-political posts and around 200 comments posted by work colleagues. For this job, Savchuk' salary was $777 a month.

Conclusions

With the proper tools, adequate human resources and a generous budget, online aggression, even it is called cyberbullying, cyberstalking or hate speech and irrespective of its ideological roots, can be speculated by entities interested in generating short-term or medium-term social tensions or animosities among supporters of diverging political trends, with direct impact on the occurrence of violent incidents, and in the long run lead to a rift between governors and citizens, or even to social disorder and dilution of the rule of law.

References:

1. Active Watch, Romani CRISS, (2016), *Raport anual cu privire la discursul instigator la ură din România 2014-2015*, available at: http://www.activewatch.ro/Assets/Upload/files/Raport%20anual%20cu%20privire%20la%20discursul%20instigator%20la%20ura%202014%20-%202015(1).pdf.

2. Apuzzo M., LaFraniere S., (2018), "13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign", *New York Times*, Feb. 16, 2018, accessed 12.09.2018 at https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html.

3. Back, M. D., Stopfer, J. M., Vazire, S., Gaddis, S., Schmukle, S. C., Egloff, B., & Gosling, S. D. (2010). Facebook profiles reflect actual personality, not self-idealization. *Psychological Science*, 21(3), 372-374. http://dx.doi.org/10.1177/0956797609360756.

4. Bargh, J.A., & McKenna, K.Y.A., (2004), "The Internet and social life, Annual Review of Psychology, nr.55, pp. 573-590.

5. Blair, J., (2003), "New breed of bullies torment their peers on the Internet", Education Week, nr.22 (1), pp. 6-7.

6. Centre for Monitoring and Combating Anti-Semitism in Romania (MCA Romania), (2015), Monitoring Report 2009-2014, available in Romanian language only at: http://antisemitism.ro/wp-content/uploads/2015/05/MCA-Romania-Raport-de-Monitorizare-2009-2014.pdf.

7. Chan, Jason, Ghose, Anindya, Seamans, Robert, (2016), "The Internet and Hate Crime: Offline Spillovers from Online Access", MIS Quarterly, vol. 40, nr.2, pp. 381-403.

8. Chen A., "The Agency", in *New York Times*, June 2, 2015, accessed 12.09.2018 at https://www.nytimes.com/2015/06/07/magazine/the-agency.html?mcubz=0.

9. Citron, D., (2014), *Hate Crimes in Cyberspace*, Cambridge: Harvard University Press.

10. Cole, Mike, (2016), "Imperialism and Racialised World Capitalism or Intercultural Twenty-First Century Socialism", Knowledge Cultures no. 4(6) pp.228–249.

11. Foran C., (2018), "GOP lawmaker: Russian meddling fanned the flames in Charlottesville", *CNN*, August 12, accessed 12.09.2018 at https://edition.cnn.com/2018/08/11/politics/charlottesville-russia-meddling-republican-lawmaker/index.html.

12. Frenkel S., Benner K., (2018), "To Stir Discord in 2016, Russians Turned Most Often to Facebook", *New York Times*, February 17, accessed 10.09.2018 at https://www.nytimes.com/2018/02/17/technology/indictment-russian-tech-facebook.html.

13. Hodges, E., & Perry, D., (1999), "Personal and interpersonal antecedents and consequences of victimization by peers", Journal of Personality Social Psychology, nr.76, pp.677-685.

14. Hu E., Brooks H., (2018), "When Radical Online Political Speech Transitions to Physical Violence", *Pacific Standard*, August 24, accessed 10.09.2018, at https://psmag.com/social-justice/when-radical-speech-gets-physical.

15. Jaishankar, K., (2008), "Cyber Hate: Antisocial networking in the Internet, International Journal of Cyber Criminology, no. 2(2), pp. 16-20.

16. Keipi, Teo, Matti Näsi, Atte Oksanen, Pekka Räsänen, (2017), *Online Hate and Harmful Content: Cross-National Perspectives*, London and New York: Routledge.

17. Michel C., (2018), "New database shows how Russian tweets inflamed tensions around Charlottesville", *ThinkProgress*, August 13, accessed 10.09.2018 at https://thinkprogress.org/new-database-shows-how-russian-tweets-inflamed-tensions-around-charlottesville-a2bff1f482d2/.

18. Parfitt T., (2015), "My life as a pro-Putin propagandist in Russia's secret 'troll factory'", The Telegraph, June 24, accessed 12.09.2018 at https://www.telegraph.co.uk/news/worldnews/europe/russia/11656043/My-life-as-a-pro-Putin-propagandist-in-Russias-secret-troll-factory.html.

19. Patchin, J.W., Hinduja, S., (2015), *Bullying Beyond the Schoolyard*, Corwin Press/SAGE Publications.

20. Patchin, J.W., Hinduja, S., (2016), *Bullying Today. Bullet Points and Best Practices*, Corwin Press/SAGE Publications.

21. Patchin, J.W., Hinduja, S., (2015), *Defining Cyberbullying: Implications for Research. Aggression and Violent Behaviour*, Corwin Press/SAGE Publications.

22. Popescu, Gheorghe H., (2016), "Does Economic Growth Bring About Increased Happiness?", Journal of Self-Governance and Management Economics nr.4(4) pp. 27–33.

23. Warzel C., (2017), "New Charts Show What The Russian Troll @TEN_GOP Account Was Tweeting This Summer", *BuzzFeedNews*, October 24, accessed 10.09.2018 at https://www.buzzfeednews.com/article/charliewarzel/new-charts-show-what-the-russian-troll-tengop-account-was.

24. Weede, Erich, (2017), "Geopolitics, Institutions, and Economics: On the Rise and Decline of Civilizations", Geopolitics, History, and International Relations no. 8(1) pp.177–220, 201.

25. Wong Q., (2017), "How Facebook is Tackling Hate Speech after the Charlottesville Rally", *Mercury News*, August 15, accessed 10.09.2018 at https://www.mercurynews.com/2017/08/15/how-facebook-is-tackling-hate-speech-after-the-charlottesville-rally/.\

26. ***, "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements", The website of the Permanent Select Committee on Intelligence of The U.S. House Of Representatives, accessed 12.09.2018 at https://democrats-intelligence.house.gov/social-media-content/default.aspx

HISTORY AND MEMORY IN INTELLIGENCE

SOVIET ESPIONAGE ACTIONS AGAINST ROMANIA IN THE FIRST INTERWAR DECADE. THE CASE STUDY OF GENERAL LUDOVIC MIRCESCU

Ioan Codruț LUCINESCU*

Abstract

"World War I destroyed a world" were the words used by a known politician, Constantin Argetoianu, in order to summarise the post-war reality. Even if only four years went by, mankind was completely different in 1918 compared to 1914. Romania is a good example for this situation, as it managed to fulfil the goal of taking back some territories that were under Russian and Austro-Hungarian dominance.

In the post-war international context, Romania had to face a double challenge: on one hand, integrating its new provinces from an institutional – administrative and economic point of view. On the other hand, ensuring a normal state of security considering that the eastern, western and southern borders were subject to Soviet, Hungarian and Bulgarian revisionism. However, the greatest threat to the state's integrity is going to be Soviet Russia who did not accept the fall of the Russian Empire. That is why, in the 3rd and 4th decades of the 20th century, it tried to destabilize Romania through every means, including aggressive espionage against the defence and security system. Although Romanian intelligence structures obliterated most of the Russian espionage networks, there were failures as well.

This study presents the case of General Ludovic Mircescu, war minister in the '20's; a case which delivered a shock to the Romanian public of that time. The Russian secret services, through a thoroughly organized action, managed to steal the Romanian plans for a war against Russia (important military documents, troops' position and movement, military structure etc.) This "wake up call" led to an unprecedented consolidation of the Romanian secret services in the following decade, with spectacular results in the fight with the Russian agents.

Keywords: *Romanian Army, secret services, Soviet Russia, interwar period*.

* Researcher, "Mihai Viteazul" National Intelligence Academy.

Introduction

In the European context at the end of WWI, Romania, as one of the dynamic actors of the international system created through the peace treaties of Versailles and Trianon (1918-1923) 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.

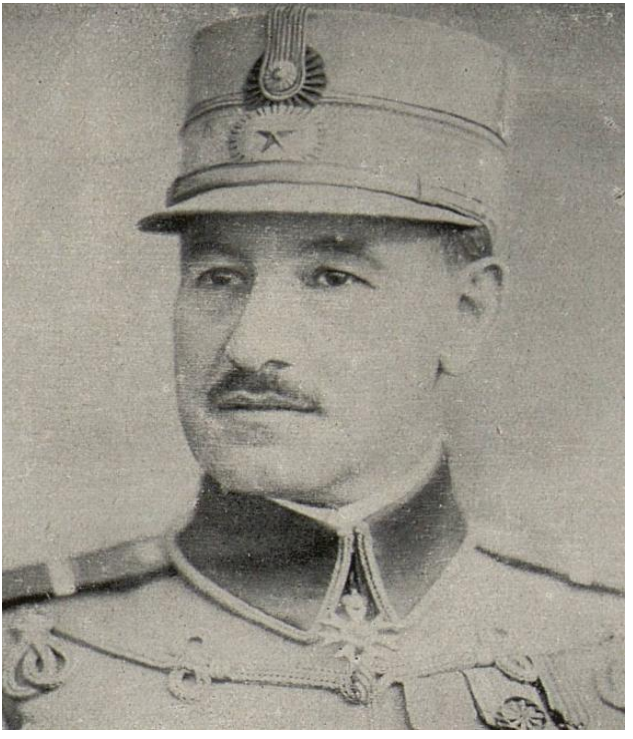
Beyond the revolutionary propaganda which excited millions of people from the former Soviet Empire, the communist leadership adopted an obviously repressive policy once it took over Russia. Denying the people's right to decide their own faith resulted in territorial loss, between 1917-1918, which was 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, 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).

However, in order to achieve this strategic objective, the significant weakening of Romania's capacity to react by internal destabilization, terror, assassinations, communist propaganda had to be achieved

A difficult and extremely tense period followed for the national intelligence structures (firstly the military ones), said services having to, in the middle of the 3rd interwar decade, face an capable and aggressive adversary, Russian secret services – VECHEKA, subsequently GPU and OGPU, (Mitrokhin, 2008), in the difficult conditions 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).

A spectacular achievement of Soviet espionage in the mid-1920s. The case study of General Ludovic Mircescu



General Ludovic Mircescu (1872 – 1930)[1]

In the first interwar decade, soviet espionage operations against the state's institutions are 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.

One of the greatest achievements of interwar Soviet espionage against Romania consists of the so-called "Ludovic Mircescu Case" – since going public it created a shock in the national public, forcing King Carol II to initiate a thorough investigation concerning the leadership of the Romanian Army. This case study revolves a mainly around the information provided in Case

[1] General Ludovic Mircescu was an appreciated senior officer – cavalry brigade commander during the First World War, then commander of Romanian Gendarmerie in 1918-1919. In the following years, his achievements in Romanian Army will culminate with appointment as War Minister (March 1926 – June 1927).

File no. 1/1927, titled *Ludovic Mircescu General Case*, which can be found at the Romanian National Archives (Police General Directorate Collection, file no. 1/1927).

The "Ludovic Mircescu Case" is about the theft of important documents regarding Romania's security, as said documents contained, in over 100 pages, details military plans, inventory, a possible move against Russia that would've taken place in Bessarabia etc. It was a professional espionage action, Russia gaining information, in detail about, the Romanian military potential; the situation was even more difficult considering that Russia thought of Romania as an enemy that had to be defeated through any means (the territorial union, that happened in 1918, between Romania and Bessarabia was viewed as an act of war by the communist authorities).

The Soviet accomplishment in the "secret frontline" happened in the summer of 1926, when cavalry General Ludovic Mircescu, War Minister, spent his time off with his mistress (a Slavic girl known as Gerda) at the Vatra Dornei resort. Ignoring the rules required to handle secret documents, the general orders the Deployment Plan to be fetched, with its detailed appendages, sketches, and graphics. All these documents were stolen by his partner, later revealed (by Romanian counterintelligence) to be an agent of the soviet secret services (Ştefănescu, 2007, p. 79). The investigation launched when the event went public reveals that the soviet secret services began the infiltration of Gerda years before, in 1920, when General Mircescu was at Cernăuți (Bukovina) as a commander of the 8th infantry division. It was, after all, a classic espionage movement, in the "honey trap" category, perfectly thought and executed, because Gerda and the accomplices left the country in the shortest time possible, without leaving a trace behind.

Although the disappearance of the documents was discovered less than a day after happening, the Romanian superior military authorities tried to cover it up and succeeding for a period of three years. But, as information about the spectacular Soviet action started showing up in both international and Romanian press, details started to unveil. Bucharest based newspapers provide large columns, describing it as the gravest espionage act against Romania.

The first information to confirm that the documents were stolen by the Soviets comes from the Secret Intelligence Service (SIS), which demonstrates the existing collaboration between the Romanian and English secret services.

In this sense, we present the information memorandum from 27 March 1927, by the Intelligence Service, addressed to the Romanian Secret Service, which confirms the theft of military documents by Soviet agents.

"Our Secret Information Service from Moscow informed us that in March, of the current year, the Soviet Special Information Service from Vienna filed an important document regarding the Deployment Plan of the Romanian Army, supplemented by a translation, from Romanian to Russian, for which the Soviets paid 25.000 schillings.

We add the following:

1. Russian military experts established that the document is real, based on their expertise.

2. The communication of our Information Service from Moscow must be considered to be real and beyond any suspicion.

28. III. 1927" (NARCollection the Precedency of the Council of Ministries – Special Information Service, File no. 1/1927, f. 2)

The document forwarded by the Intelligence Service to the Romanian Secret Service proves the valuable information network owned by the British inside Russia, despite the OGPU's extreme measures in order to make the foreign secret services activity on Soviet ground useless.

Echoes of the case in the public

The press thinks about the "Mircescu Case" as being the worst espionage act against Romania until that moment. Thus, "Ordinea" newspaper, no. 534 from 17th September 1930 says, in capital letters: "We are around a never-before-seen military scandal. After some disclosures in the Russian and German press, it wouldn't be surprising for resignation letters to be required from a former War Minister and his former General Secretary, both active generals in the army.

It is said that due to some grave dereliction of duty, both the army's and the country's interests had a lot to suffer. What happened unveiled a terrific intelligence network that the country's memoirs use to surround it ..."

The news, as it gained information from local and foreign sources, highlighted a novelty fact – the collaboration between Russian and German secret services in order to spy on Romania, because agent Gerda was working for both of them, as it was established by Romanian and British secret services (also informing the press).

The Russian-German informative collaboration emerges from another document belonging to the Secret Services, addressed to the military. Both

Russia and Germany were after the annulment of the peace treaties signed at the end of World War I.

"SECRET DOCUMENT

I. The history of the problem

The General Staff were notified by the British, through the Foreign Office, that the 1926 Romanian Deployment Plan was stolen. This document was given by the state to the adjutant general Florescu M. Ioan to be presented to the Minister of National Defence (General Mircescu Ludvig).

Spy 48 R., from Cernăuți (Chernivtsi)-presently in the service of Germany and of the OGPU, stole it.

II. People involved

- General Mircescu Ludvig (deceased)
- Adjutant general Florescu B. Ioan (deceased)
-Spy 48 R.

III. Conclusions

Immediate change of the Romanian Deployment Plan and its appendages.

IV. Proposals

Documents of such importance are not to be studied outside the state or the Ministry of National Defence" (NAR, Collection the Precedency of the Council of Ministries – Special Information Service, File no. 1/1927, f. 48).

The denouement was tragic, the army's honour badly affected, which drove King Carol II to order General Ludovic Mircescu – urgently summoned, in the autumn of 1930, from Paris – to take the decision of defending his military honour (taking his own life).

In this way, in November of 1930, the newspapers announce the death of general Mircescu "after a long-suffering", circumstance in which he is presented with eulogies concerning his activity as a soldier with important army leading duties.

Conclusion

Acknowledging the danger of soviet espionage following this massive scandal lead to an obvious improvement, in the following years, in the activity

of the national intelligence services through the allocation of superior financial resources, a broad staff upgrading process etc.

The intelligence activity of the Romanian secret services in the interwar period resulted in:

- Neutralizing the complex actions launched by neighbouring revisionist states aimed to Destabilize Romania.
- The absence of a strong communist party on the Romanian territory up to the end of World War II.
- A correct informational flow to the superior national decision-making levels, concerning threats to national security.

At the same time, the need to make the intelligence structures more effective and to organize a modern intelligence service (The Secret Intelligence Service) to counteract the whole range of threats to national security, either from the West or from the East, was felt.

References:

1. National Archives of Romania, Collection Police General Directorate and Collection the Precedency of the Council of Ministries.
2. Constantiniu, Laurențiu, (2010), *Uniunea Sovietică între obsesia securității și insecurității*, Editura Corint, București.
3. Mitrokhin, Vasiliy, (2008), *"CHEKISM". Tales of the CHEKA, A KGB Anthology*, The Yurasov Press, London.
4. Moraru, Pavel, (2008), *Serviciile secrete și Basarabia (1918 - 1991)*, Editura Militară, Bucureşti.
5. Ştefănescu, Paul, (2007), *Istoria serviciilor secrete române*, Editura ANTET, Prahova.
6. Volodarski, Boris, (2015), *Cazul ORLOV. Dosare KGB*, Editura Litera, Bucureşti.
7. Troncotă, Cristian, (2004), *Mihail Moruzov și frontul secret*, Editura ELION, Bucureşti.
8. Troncotă, Cristian, (2008), *România și frontul secret 1859 – 1945*, Editura ELION, Bucureşti.

THE IMPORTANCE OF THE ACTIVE MEASURES PROGRAM WITHIN THE COLLABORATION AND INTELLIGENCE SHARING AMONG WARSAW TREATY ORGANIZATION MEMBER STATES' SECURITY AND INTELLIGENCE SERVICES AGAINST THE WEST AND NATO ALLIES DURING THE COLD WAR

Mircea STAN[*]
Florin BUȘTIUC[*]

Abstract

The article analyses the impact of the active measures program within the collaboration and information exchanges among Warsaw Treaty Organization member states' security and intelligence services against the West and NATO allies during the Cold War. The active measures conceived by the Soviets have been and still are truly sophisticated instruments that generate strategic events with the aim of creating advantages on short, mid and long term. The Soviet active measures program was an integrated part of the Warsaw Treaty Organization members' security and intelligence services collaboration against what was known as a common enemy, the West and NATO.

From the very eve of institutionalized intelligence/counter intelligence structures the cooperation and information sharing were a necessity for gathering information. The fall of the Iron Curtain over Europe was the start of a race between security and intelligence services from East and West. The successful operations of the Warsaw Treaty members against the West and NATO were partly due to the cooperation of their security and intelligence structures, and a very important role was played by the active measures program.

The working hypotheses are: the insufficient studies dedicated to the subject and the importance of the active measures for the past, present and future of the security and intelligence services; declassification and further possibility of studying documents relevant for the topic; the importance of bilateral and multilateral cooperation and information sharing during the Cold War inside the Warsaw Treaty Organization; the extent of the active measures program in the field of cooperation and information sharing.

[*] Phd "Mihai Viteazul" National Intelligence Academy, stanmircea90@gmail.com.
[*] Expert "Mihai Viteazul" National Intelligence Academy, florinnn11@yahoo.com.

Keywords: *active measures program, security, intelligence, counterintelligence, espionage, inter-institutional cooperation, information sharing, diplomacy*.

Soviet and American perspectives on the taxonomy of the active measures program in different historical contexts

Active measures (**activnyye meropriyatiya**) are a term used in the Soviet jargon specific for security and intelligence services. Its origins can be traced back before the USSR even existed and it has been used in promoting Russian/Soviet interests beyond its borders. The origin of the concept can be found in the Czarist period, being closely linked to two security institutions whose main objective was controlling the civil society: the Third Section of His Imperial Majesty's Own Chancellery and the Okhrana.

The failed revolution in 1825 determined Czar Nicholas I (1825-1855, crowned in 1826) to establish the Third Section of His Imperial Majesty's Own Chancellery (**Tret'ye otdeleniye Sobstvennoy Yego Imperatorskogo Velichestva kantselyarii**) (Monas, 1961, p. 63). The chief of this structure was Count Alexander Konstantinovici Benckendorff. A handkerchief given by the Czar and kept in a glass box was the symbol of the Third Section. According to tradition, Czar Nicholas I told Benckendorff: "Here are all the instructions. The more tears will be wiped out with this handkerchief, the better I will serve my purposes" (Andrew and Gordievski, 1994, p. 16). Therefore, at that time, the Third Section used to be the "moral doctor" of the Russian society. The main objective of this structure was to control the public opinion.

A relevant landmark in Nicholas I's reign is an act that „instituţionalizase crima politică". The 1845 "The Criminal Code" provided for tough sanctions on "the persons guilty of spreading handwritten or printed material or manifestations intended to induce a lack of respect for the sovereign authority or the sovereign qualities or its government" (Andrew and Gordievski, 1994, p. 17).

In August 1880, the Third Section was disbanded and replaced by the Department of the State Police whose name changed to Police Department in 1883. The "responsibility" of political crime was transferred to the Special Section (**Osobîi Otdel**) and a network of security sections called (**Ohrannoe otdelenie**) (Andrew and Gordievski, 1994, p. 17-18). The first such section was founded in 1880 under the name Okhranka – the Department for Defense of Public Security and Order (**Otdelenie po ohraneniiu obşcestvennoi bezopasnosti i poriadka**), also called the Defense Department (**Ohrannoe otdelenie**) (Encyclopaedia Britanica). The Okhranka had two defining aspects: a) back then it was a unique institutionalized structure in Europe due

to its form of organization, activities, duties and responsibility to protect tsarism; b) it contributed decisively to the implementation of state anti-Semitism. The Okhranka was abolished together with tsarism in February 1917, a first step towards the Bolshevik Revolution in October 1917.

Both the Third Section and the Okhranka conducted their active measures programs in order to prevent the overthrow of monarchy. They had done so by controlling the population inside the state borders and penetrating dissident groups. A well-known case involved dissidents from France (Hingley, 1971, p. 80). So far, influence, subversion, manipulation (Shultz and Godson, 1984, p. 2) were the most common methods used to implement the active measures programs. The information is confirmed by a second source which adds three more elements: penetration, instigation and deception (Dziak, 1987, p. 39).

Thus far it can be argued that active measures programs used to have a more internal focus, therefore they belonged to what we may call in a more modern sense, counterintelligence[1] and they included six elements: influence, subversion, manipulation, penetration, provocation, deception. (Dziak, 1987, p. 39) After the Bolshevik Revolution and the establishment of Cheka (**Vserossiyskaya chrezvychaynaya komissiya** – the All-Russian Extraordinary Commission for Combating Counterrevolution and Sabotage, 1917-1922), the new regime was faced with a severe lack of legitimacy. In order to fill this vacuum, a new bureau, meant to spread disinformation, was established within the GPU (**Gosudarstvennoye politicheskoye upravlenie** – the Soviet State Political Directorate from 1922 until 1923) "to stifle counter-revolutionary movements of enemies". This type of actions will be gradually amplified during the interwar period, with a special focus on chasing former dissidents, especially Leon Trotsky (Pringle, 2006, p. 3).

A constant aspect can be attributed to the program of active measures: its place in the field of Czarist/Russian/Soviet counterintelligence. Furthermore, we can add disinformation to the six elements specific to the active measures programs.

In the "KGB Lexicon", therefore after 1954, active measures were included in counterintelligence jargon, being defined as activities undertaken by counterintelligence services in order to prevent undesirable outcomes that could affect the internal order. The offensive potential of counterintelligence

[1] It must be mentioned that the active measures program initially played a defensive role (its activities were mostly limited within the borders of the Czarist empires) but it also included an offensive component meant to penetrate, intoxicate and influence the dissident groups active outside the Empire's borders.

was underlined, namely the prevention of (possible) hostile activities undertaken by (potential) opponents in the field of intelligence (Mitrokhin, 2004, p. 251).

After the Second World War, the active measures program became more significant for the Soviets as special emphasis was placed on disinformation. For this reason, in 1959, Department "D" (**Dezinformatsia)** was established within the PGU (**Pervoe Glavnoe Upravlenie** – the First Main/Central Directorate – Foreign Intelligence, soviet espionage, 1954-1991) and tasked with taking over and implementing all the active measures operations[2].

On a side note, secret/undercover operations were counterparts to the Soviet program of active measures, although it needs to be mentioned that the latter included a much wider range of secret/undercover activities, while also being known for "open and secret techniques applied to influence the events, strategies and actions of other countries" (Richard H. Shultz and Roy Godson, 1984, p. 193).

Cristopher Andrew and Vasili Mitrokhin define active measures as a means of influencing world events according to KGB interests "(...) ranging from media manipulation to «special actions» involving various degrees of violence" (Andrew and Mitrokhin, 2001, p. 224).

During the hearings before the US House Permanent Select Committee on Intelligence in July 1982, active measures were defined as follows: "The Soviet term active measures is used (primarily in an intelligence context) to distinguish influence operations from espionage and counterintelligence, but this term is not limited to intelligence alone . . . involve activities from virtually every element of the Soviet party and state structure and are regarded as a valuable, regular supplement to, and are closely coordinated with, traditional diplomacy. Soviet active measures include: Manipulation or control of the media; Written or oral disinformation; Use of foreign Communist parties and front organizations; Clandestine radio broadcasting; Economic activities; Military operations; Other political influence operations" (The Congress of the USA, July 13 and 14, 1982, p. 1).

---

[2] There is conflicting data regarding the establishment of Department "D". Some sources support a version in which Service "A" (Slujba Aktivnik Meropriatil or the Service of Active Measures) became the successor of Department "D" (Dezinformatsia) in 1962. (See: Watts, 2011, p. 302) Other sources indicate that Service "A" became the successor of the Department "D" in 1971, at a time when the department included 700 officers and a KGB (Komitet Gosudarstvennoi Bezopasnosti – USSR's Committee for State Security, 1954-1991) general was in charge of it. (See: Schoen and Lamb, June 2012, p. 19)

The same document mentions that "Soviet active measures constitute a policy instrument systematically employed to discredit, isolate, and weaken the United States. These ultimate objectives are a key factor in active measures, even in many instances when the active measures are immediately directed at other countries, organizations, or individuals". (The Congress of the USA, July 13 and 14, 1982, p. 1)

From another perspective, active measures can be described as "A Soviet term that came into use in the 1950s to describe certain overt and covert techniques for influencing events and behaviour in, and the actions of, foreign countries. Active measures may entail influencing the policies of another government, undermining confidence in its leaders and institutions, disrupting relations between other nations, and discrediting and weakening governmental and non-governmental opponents. This frequently involves attempts to deceive the target (foreign governmental and non-governmental elites or mass audiences), and to distort the target's perceptions of reality. Active measures may be conducted overtly through officially sponsored foreign propaganda channels, diplomatic relations, and cultural diplomacy. Covert political techniques include the use of covert propaganda, oral and written disinformation, agents of influence, clandestine radios, and international front organizations. Although active measures principally are political in nature, military manoeuvres and paramilitary assistance to insurgents and terrorists also may be involved". (Shultz and Godson, 1984, p. 193)

From the point of a view of a former Central Intelligence Agency (CIA), "Active Measures were clandestine actions designed on the one hand to affect foreign governments, groups and influential individuals in ways favouring the objectives of Soviet policy and, on the other hand, to weaken the opposition to it. Such actions might or might not involve misinforming an adversary by distortion, concealment or invention, but in practice we got better results by exposing truth – selectively. We usually made the distinction clear. When someone would propose a measure, for instance, we would frequently ask him, «How much deza [disinformation] is involved in it? »". (Clizbe, 1999, p. 99).

Oleg Danilovici Kalughin (former director of PGU's external counterintelligence directorate) described active measures as „inima și sufletul informațiilor sovietice": "Not intelligence collection, but subversion: active measures to weaken the West, to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people of Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs" (Kalugin, January 1998).

By analyzing these sources, the active measures program during the Cold War can be defined as a range of sophisticated methods (disinformation, subversion, influence, propaganda, undercover operations, deception, rumours, manipulation, provocation, forgeries, diversion, **maskirovka**, reflexive control, sabotage, penetration, discreditation) which generate strategic events in order to gain short, medium and long-term advantages in social, political, military, economic and intelligence terms.

Mechanisms of implementing the program of active measures

Going back to the World War II security and intelligence services, the first chief of Department "D"/ Service "A" (starting in 1966) of the PGU was Ivan Ivanovich Agayants (code name "Avlov", he was MGB[3]/KI[4] resident in Paris between 1947-1949). He headed the structure between 1959 and 1967. The next chief was Alexandrovici Kondracev[5] (1967-1968), followed by Nikolai Antonovici Kosov (1968-1976), Vladimir Petrovici Ivanov (1976-1990), Leonid Alexeevici Makarov (1991-). Service "A" contained four directorates: political, economic, political-military and operational[6].

The mechanism of cooperation for implementing the program of active measures followed this path: Department "D"/Service "A" worked with the Foreign Affairs Section of the Central Committee of the Communist Party of the Soviet Union (CC of the CPSU)/Foreign Affairs Sections of the Central Committees of the other communist parties in socialist countries, the Propaganda Section of the CC of the CPSU/Propaganda Sections of the other communist parties in socialist countries, the Soviet Academy of Science/Science Academies of the other socialist countries, the PGU residences and the written and audiovisual press.

Within PGU residences, the mechanism of cooperation was provided by the "PR Line", which was in charge of economic and political information, military strategy and active measures (Mitrokihn and Andrew, 2003, pp. 454, 476, 570). According to a former officer of Service "A", who defected to the

[3] MGB – Ministerstvo gosudarstvennoy bezopasnosti – USSR's Ministry of State Security between 1946 and 1953 (Andrew and Gordievski, 2001, p. XVII; Mitrokihn and Andrew, 2003, p. 9 and 2006, p. 14).

[4] Komitet Informații – Soviet intelligence agency between 1947 and 1953. Initially, it integrated various foreign intelligence directorates from MGB and GRU (Glavnoe Razvedîvatelnoe Upravlenie – the Soviet military espionage service or the Main Intelligence Directorate), (Mitrokihn and Andrew, 2003, pp. 8 and 14 and 2006).

[5] Some authors argue that he became chief of Service "A" in 1970 (Volkoff, 2000, p. 14).

[6] Available at: http://shieldandsword.mozohin.ru/kgb5491/structure/1GU/A.htm, accessed on [19.07.2018].

USA in 1979, the active measures program was not implemented outside the Soviet borders by Service "A" officers. Instead, this mission was given to the "PR Line" staff along with precise instructions. Also, Service "A" used to draft a bulletin which contained secret information. The bulletin was given to the members of the CPSU Politburo. It included specific details of certain active measures programs or other operations that were already successfully implemented (Barron, 1983, p. 449).

Department "D" also used to cooperate with the residencies of security and intelligence services of other socialist countries, the Foreign Affairs Sections and the Academies of Science of those respective states. However, no actions were ever performed outside of KGB orders (Knight, 1990, p. 286).

Throughout the Cold War, the USSR had the advantage of receiving the support of powerful socialist parties in Western countries, especially France and Italy. The implementation of active measures was supported by Soviet advisers (Bittman, 1972, p. 45) placed in intelligence and military structures and the Cominform (1946-1956)[7]. After the dissolution of the latter, the same role was given to the Foreign Affairs Sections of communist and working-class parties in socialist countries.

Disinformation, **maskirovka**[8], provocation, penetration, forgery, diversion, influence agents, conspiracy, wet affairs and combination (Dziak, 1987, pp. 39-40) were the best-known elements of the active measures program from the establishment of Cheka until the seventies.

Between 1959 and 1965, the KGB "exported" its program of active measures to the other security and intelligence services of the Warsaw Pact (WP) member states (Bittman, 1985, pp. 142, 156-157) except Romania.

For example, the 1960 organization structure of the KDS (**Komitet za Dăržavna Sigurnost** – the Bulgarian State Security) mentions the Sixth

[7] It was founded on September 22th 1947. Its headquarters was in Belgrad. The Cominform had to ensure that links were created between European communist and working-class parties. It was designed like an "Information Office of Communist and Workers' Parties". The Cominform had lots of information on how the "popular democracies" were established. (Duroselle, 2006, p. 352)

[8] A traditional Soviet term used in military operations. Maskirovka is a term used to describe a "mix" of deception, hiding, simulation, disinformation, false demonstration, camouflage, all meant to hide the real position of the troops and mislead the enemy, leading to inaccurate plans, forecasts and conclusions. (Pirnie, 1985, pp. 1-22; Keating, 1981, pp. 1-20). In the KGB jargon, maskirovka describes a larger set of intelligence/counterintelligence actions such as: camouflage in surveillance (maskirovka v naruzhnom nablyudenii), camouflage of clandestine radio communication (maskirovka konspirativnoy radiosvyazi), and camouflage of microdot (maskirovka mikrotochki) – it refers to a small text or image printed on a disc to prevent its detection (Mitrokhin, 2003, pp. 64-68).

Department (within the Foreign Intelligence Directorate), a structure involved in disinformation operations (Persak and Kamiński, 2005 , p. 39). On November 17th 1967, by virtue of order I-3728, the Sixth Directorate for "«combating the ideological subversion of the enemy»"(implying "«ideological imperialist subversion and propaganda»") was established. The Sixth Directorate contained eight departments (Persak and Kamiński, 2005, p. 44).

We can observe that the Bulgarian active measures program was based on three components: disinformation, subversion and propaganda. Also, the KDS and the KGB worked together in a program of active measures that was focused on two major cases: "Bulagarian umbrella" in London, September 1978 and "Bulgarian connection", an attempt to assassinate Pope John Paul II (Persak and Kamiński, 2005, p. 69).

Regarding Czechoslovakia, the Eighth or "D" Department was founded in February 1964. It was unofficially called the department for active measures or disinformation. According to Ladislav Bittman[9], the Eighth Department was involved in 115 active measures operations in 1965 and 300-400 of these were performed every year by all WP countries – except Romania (Bittman, 1972, p. 16 and 1985, p. 39). Bittman also argues that in the early stages of active measures departments three elements were very common: disinformation, propaganda and influence (Bittman, 1972, p. 20).

In Poland, the active measures program began with the establishment of the Independent Group "D" (disintegration and disinformation) on November 19th 1973, a direct order of Stanisław Kowalczyk (1973-1980), the MSW (**Ministerstwo Spraw Wewnętrznych** – the Ministry of Internal Affairs). Initially, Independent Group "D" functioned within the Fourth Department (its responsibilities were related to the Catholic Church and other religious organizations) but later it was reorganized into a separate department (the Sixth Department) inside MSW. The operations of the Independent Group "D" were kept secret even from the other SB officers who worked in other departments. The staff involved in the operations did not record any detailed documentation related to their activity. At the time, the activity of the Independent Group "D" was not compatible with the Polish legislation (Persak and Kamiński, 2005, pp. 221-283).

Colonel Konrad Straszewski and four other SB (**Służba Bezpieczeństwa** – the Polish State Security) officers played a major role in

[9] Defector from the StB (Státní Bezpečnost – the Czechoslovak State Security). Between 1954 and 1968 he worked in Czechoslovak espionage. Between 1964 and 1966 he headed the Eighth Department. See Ladislav Bittman, *op. cit.,* pp. IX-XXV. Bohumír Molnár was Ladislav Bittman's successor as chief of the Eighth Department. See: Persak and Kamiński, 2005 , p. 161.

founding the Independent Group "D". Disintegration and disinformation activities were based on strategic and tactical hypotheses that were previously elaborated. The chiefs of the Independent Group "D" were Zenon Płatek (1974-1976), Tadeusz Grunwald (1976-1982), Grzegorz Piotrowski (1982-1983), Wiesław Fenicki (1982-1983), Romuald Będziak (1983-1984) și Robert Szczepański (Pleskot, 2016, pp. 214-215).

Between November 18th and November 22nd, Konrad Straszewski led a group that travelled to Moscow to sign "Joint Operational Plan"of MSW's Fourth Department and the KGB. The aim of this agreement was to fight against the subversive activity of the Catholic Church and the Vatican (Lasota, 2003, p. 51). Cooperation between the KGB and the SB was very active. The KGB used the SB to implement its program of active measures. Many SB officers who worked in the Independent Group maintained unofficial ties to the KGB (Grajewski, 2008, pp. 177-198).

In terms of active measures, the USSR's partnership with Hungary produced the best results among Eastern Bloc states. After the 1956 Revolution, ÁVH (**Államvédelmi Hatóság** – The Hungarian State Security between 1948 and 1956) was disbanded. Hungarian security and intelligence services were reduced to a single directorate (the Third Directorate) within the Hungarian Ministry of Interior (Gábor, 2013, p. 36). Several independent departments worked within the Third Directorate. The first one used to deal with foreign intelligence. Available documents confirm the fact that a department of active measures had functioned within the Foreign Intelligence Department between 1964 and the end of the communist regime in Hungary: between May 1964 – August 1967, "Evaluation and Information Department" – active measures; August 1967 – July 1971, Department VII – active measures; July 1971 – 1980, Department VII – active measures. Active measures were performed by using disinformation, propaganda, psychological actions, subversion and they were used to destabilize emigrants' organizations as well as other international organizations such as NATO, CIA and BND (**Bundesnachrichtendienst** – Germany's Federal Intelligence Service) (Eszter, 2011, pp. 1-25).

Active measures received special attention in documents drafted by the Hungarian Ministry of Interior. At least around 1969, they mentioned people, bodies or subjects. The documents contained information concerning files that were related to active measures, where they were stored, and additional details about the implementation itself (Belügyminisztérium, 1969, pp. 3-51).

Regarding GDR (the German Democratic Republic), active measures were first implemented in 1956 by a small group of people. Department X of

the HV A. (**Hauptverwaltung A. – Aufklärung**, East German espionage headquarters A) was initially responsible. The purpose of GDR's active measures was to weaken the international position of the Federal Republic of Germany (FRG), established by the Hallestein Doctrine[10]. This meant influencing Western Europe and USA mass-media according to policies established at the level of the Socialist Bloc (Wolf and McElvoy, 1998, pp. 233-234; Münkel, 2015, pp. 143-144). HV A.'s Department for Mobilisation, "Domestic Security", Evaluation of Foreign Counter – Intelligence, "Active Measures" (Persak and Kamiński, 2005, p. 172; Olaru and Herbstritt, 2005, p. 434) appeared in the 1989 MfS (**Ministerium für Staatssicherheit** – the Ministry for State Security) organization structure. The department was headed by Colonel Rolf Wagenbreth and he was assisted by his two deputies: Colonel Wolgand Mutz (First Deputy) and Colonel Rolf Robe (Wiedmann, 1996, p. 356). In 1989, MfS' active measures program was based on disinformation and publishing material, financial support for influence agents and journalists focused primarily on the FRG (Wiedmann, 1996).

Romania was excluded from KGB's program of transformation at the level of security and intelligence services in the socialist sphere of influence, services which tended to collaborate well with the KGB. The decision to marginalize the Romanian intelligence and security services was applied as a countermeasure for the state's foreign policy. For the Securitate, this meant a greater amount of work to maintain its credibility internationally and to protect the trust between citizens and government, while preventing the Soviets from appointing their loyal people in key positions (Bittman, 1972, p. 130 and 1985, pp. 44-47).

The active measures program, an element which describes military and non-millitary irregular/unconventional methods of hybrid warfare

Wisdom begins with the definition of terms (Socrates). Considering the fact that the purpose of this article to highlight the importance of active measures in USSR's intelligence/counterintelligence activity, it is useful to present a Soviet/Russian perspective. Understanding an opponent is only possible if the analysis uses his concepts instead of our own.

Active measures were predominantly used by Soviet security and intelligence services and they also included the usage of military elements. I

[10] Named after West German politician Walter Hallstein, one of the founding father of the EU, former president of the European Commission between 1958 and 1967. The Hallstein Doctrine argued that the FRG was right in refusing to maintain diplomatic relations with any state that recognized the GDR. The doctrine was abandoned after 1970.

can now affirm that nowadays active measures can be described as an element of hybrid warfare, "a military strategy that combines elements of conventional war, unconventional and cyber war"(Dungaciu, 2017, p. 190). To clear things up, irregular/unconventional warfare is a term used to describe what we nowadays call asymmetric warfare, with similar purposes or intentions, or, in American usage, fourth generation warfare (Robinson, 2010, p. 10 and pp. 166-167).

As a preliminary conclusion, corroborating the information found in footnote no. 3 and a personal definition that has been mentioned before, the Russian Federation only transferred the active measures from the intelligence/counterintelligence field to the military one, thus highlighting a paradox with a double significance which brings memories of the Cold War East/West rivalry: 1) while one side concentrated their efforts on innovation/development, proving its authentic intentions of progress (the Western side, the strong one), the other focused on "stealing" (the Eastern side, the weak one); 2) the Soviet Union and the "states in tight cooperation" from the WP (except Romania) implemented active measures against the West because they were the weaker international political actor in the East – West power equation. However, the second significance must be understood from the following perspective, as a lesson learned: the USSR was the first one to create structural "innovations" in the military and counterintelligence field, precisely as a response to the East-West development gap which increased USSR's/Russia's state of insecurity.

From our point of view, the program of active measures is a counterpart to the irregular or unconventional warfare. In order to bring the definition of the active measures program to the present, I argue that the program of active measures describes military and non-military irregular/unconventional methods of hybrid warfare. To better understand the current implications of the active measures program, it is necessary to present a retrospective of hybrid warfare.

Despite everything that has been said, both officially and unofficially, hybrid warfare is not new. Academic literature presents Evgheni Eduardovici Messner (1891-1976)[11] as probably one of the first authors to describe this

[11] Evgheni Eduardovici Messner (1891-1976). Had a rich experience in military theory and practice, he served as an officer in the Imperial Russian Army, fighting against the Bolsheviks during the Russian Civil War (1917-1923), After this episode, he sought refuge in the Kingdom of Yugoslavia (1918-1943). He taught at the War School in Belgrad. During the Second World War he collaborated with the Wehrmacht and after the end of the war he moves to Argentina. See: Elżbieta Sawa – Czajka, „Rebel – war in Ukraine" in *The Journal of Kolegium Jagiellonskie Torunska Szkola Wyzsza*, vol. I: 25-31, 2014, p. 25.

practice. In the early 1950's, he theorized a type of warfare he called "insurrectional war" or "rebellious warfare." Messner said: "In such an armed conflict, combatants are not an army, but rather people's movements. In this case, the word "people" has no negative connotations, no one positive.

In the last decades classic warfare[12] was replaced with a rebellion type of armed conflicts with no well-defined battle fronts or opponents. Instead, psychology and propaganda are the most important elements in the preparation and evolution of these confrontations. Messner also proposed a hierarchy of objectives for this type of confrontations: a) at internal level, destroying the unity of the opposing nation, creating destabilizing situation in the army or in other institutions responsible for defending the territory and the population of the state, taking over or destroying some valuable psychological objectives; b) at external level, trying to gain new allies while weakening the support given by the enemy's allies (Sawa – Czajka, 2014, p. 26).

The concept of hybrid warfare became a topic of scientific debate after November 2005, when Frank G. Hoffman and James N. Mattis published their article "Future Warfare: The Rise of Hybrid War" (U.S. GAO, September 10, 2010, p. 18). The study of these two military theoreticians highlights several aspects: 1) future means of conflict are unpredictable; 2) the conventional threat will never disappear, therefore the USA should never lose its superiority in this field; 3) hybrid wars are caused by hybrid threats.

Nowadays there are several definitions for what we call a hybrid threat: a) an opponent which is able to use and adapt a combination of means (political, military, economical and social) and methods (conventional, unconventional, disruptive, criminal, terrorism). This type of threat can include a combination of state and non-state actors; b) a threat that uses both regulated and unregulated forces simultaneously, including terrorism and criminal elements to reach its objectives, using a variety of conventional and unconventional tactics to create more dilemmas (U.S. GAO, September 10, 2010, p. 18).

According to Hoffman, hybrid threats incorporate a complete range of different means of warfare, including conventional capabilities, unconventional tactics, terrorist acts, generalized violence, constraint and chaos (Hoffman, 2009, p. 36).

---

[12] According to experts, modern warfare has known three generations up until now. The first generation (1864-1860). The second generation is associated to the First World War, when the military thinking of the nations' armies was dominated by "massive fire power" as a key element for victory. The third generation warfare pays more attention to initiative rather than obedience (...). In the fourth generation, war "moved more to disorder and descentred power" (See: Paul Robinson, 2010, p. 166)

In the 2010 Russian Military Doctrine, modern warfare is described as the integrated use of military force and non-military resources, while the chapter "Characteristics of Contemporary Military Conflicts" highlights the high usage of military equipment systems based on psychological principles "Which are compared to nuclear weapons in terms of effectiveness"; increasing the role of the informational war and, most importantly, creating in the territory of the belligerent part of "a permanent area of military operations" (*The Military Doctrine of the Russian Federation*, 2010, p. 28).

The strategic concept of hybrid warfare or non-linear war has reshaped the new doctrine of the Russian army, while the principles it is based on are still unclear. However, according to Gherasimov, hybrid warfare involves some principles that gain mutual strength.

First, it is the concept of "permanence of the conflict", which blurs the boundaries of space and time, of war and peace and of the actors involved. Essentially, it becomes more and more difficult to determine if there is a state of war or not, especially if you are being attacked.

Second, hybrid conflicts have an emergent and multidimensional side. Political and strategically objectives are not achieved through conventional military methods anymore. Hybrid warfare forces the army and the civil population of the opponent to support the attacker to the detriment of their own country.

Third, there is "the unitary effort". The implication is that mixed tactics are applied simultaneously on the enemy's territory and more importantly in his spheres of influence.

Collaboration and intelligence sharing among Warsaw Treaty Organization member states' security and intelligence services against the west and NATO allies during the cold war.

The confrontation between the great powers, the USA and USSR had created an opportunity for security and intelligence cooperation in those states that supported one of the two ideologies. Just as the CSUP was an ideological model for the communist parties in Central and South Eastern Europe, so was the KGB for the security and intelligence services in those countries. Before presenting the terms of cooperation and the information exchanges between the security and intelligence services of the WP state

members against NATO and the West, during the Cold War[13], it is necessary to define the concepts of cooperation and information exchange.

Cooperation in the field of security and intelligence is essentially an oxymoronic concept and it can only be achieved if two or more states share the same interests and cooperation does not affect them. These interests are basically related to national security and they are linked to the sovereignty, independence and unity of an international political actor. From this perspective, cooperation is difficult to be achieved in the field of security and intelligence either bilaterally or multilaterally. However, security and intelligence cooperation already has a tradition and it is continually developing.

Within the communist system, as the most important security and intelligence service of the Warsaw Pact, KGB has developed a specific lexicon. There is the term "**razvedyvatelnoye sotrudnichestvo**" which refers to secret cooperation in active intelligence activities (Mitrokhin, 2004, p. 114).

The analysis of available documents reveals the good collaboration between the intelligence and security services of the WP countries with a sole exception, the Securitate in Romania, which did not maintain a constant level of cooperation and information exchange. Overall, the inefficiency of the collaboration between the Securitate and the other similar structures in the WP countries can be attributed to political frictions. The cooperation and information exchange between the intelligence and security services of the WP countries during the Cold War can be summarized by underlining the following stages: 1) a phase in which intelligence/counterintelligence activities were led by Soviet advisers in each socialist country along with the establishment good relations with the KGB-GRU headquarters; 2) a détente phase associated with the Brezhnev Doctrine, meant to reform the system of inter-institutional collaboration while strengthening USSR's ties with partner countries in the field of intelligence and security, however this principle did not also apply to Romania; 3) a final phase associated with the last decade of communism, in which cooperation and information exchange were further reinforced in all partner countries except Romania.

The cooperation mechanisms implemented by the KGB and GRU were either bilateral or multilateral. In the field of security and intelligence services,

[13] The term "Cold War" gets its dual paternity from the critique of Walter Lippman, American journalist and publisher, which he addressed to George Kenan in regards to his attitude towards USSR politics. At the same time, Bernard Mannes Baruch, President Roosevelt's advisor, used the term "Cold War" to describe the state of international relations. (Lippman, 2009, p. 24)

the KGB preferred bilateral collaboration in order to obtain information from each partner country. This practice did not exclude multilateral meetings.

Another cooperation mechanism could be identified at the level of the Warsaw Pact. Following the structural reforms established at the meeting in Budapest, on March 17th 1969, several structures were subordinate to the Political Consultative Committee (PCC): a) the Committee of Ministers of Defence (of WP member countries); b) the Joint Armed Forces Command (JAFC) which was in charge of the Joint Armed Forces (JAF), the (JAF) General Staff, the Military Council[14] and the Technical Committee; c) the Joint Secretariat; d) the Permanent Commission (it must be mentioned that the members of the Joint Secretariat and the Permanent Commission did not hold a public office until the next reform of the WP). The establishment of two new structures subordinate to the JAFC (the Technical Committee and the Military Council) appears as the most significant change (Fodor, 1994, pp. 35-36). The next structural reform of the WP was approved in November 1976 during the meeting of the PCC in Bucharest. Within the new structure, the Permanent Commission was replaced by the Committee of Ministers of Foreign Affairs (CMFA), while the Joint Secretariat retained the same role it had in 1956 (Fodor, 1994, p. 37). The exchange of military information was performed within these structures; since 1965, Romania was excluded from the strategy programs of the WP due to opposing views concerning foreign policy.

KGB-KDS (cooperation and information exchange in scientific and technical fields)

The KGB developed one of its most successful working relationships with the KDS. In order to highlight their partnership it could mentioned that "the basic issues of Soviet – Bulgarian post-war Security and Intelligence cooperation can be found in about 300 files from the first 22 Departmental Records at the Archive of the Ministry of the Interior in Sofia, which consist of about 27,000 pages in general. Approximately 16,000 pages of these files were Intelligence Information, Estimates, and Analyses, sent regularly by the KGB to Sofia in the period 1954–1989. Other more than 11,000 pages comprise Plans, Agreements, Protocols, Reports of meetings, and Correspondence between Soviet KGB and Bulgarian KDS services" (Baev, 2008, p. 25).

[14] The commander-in-chief, acting as president, its deputies (one from each member state) and the chief of the JAF General Staff were the members of the Military Council of the Joint Command. See ANIC, Collection *Tratatul de la Varşovia. Ministerul de Externe*, (1954-1991, and 1993), file no. 23/1966, f. 33.

The scientific and technical fields were among the most successful for the KGB-KDS partnership. An important aspect is easily noticeable: while the Western countries were separately developing their scientific research, thus creating rivalries between themselves, the Eastern Bloc countries were coordinating their activities by sharing duties. The PGU officers were leading the group, being in charge of the most important operations of scientific espionage in Eastern Europe. Declassified documents from the Bulgarian archives indicate that Bulgaria used to be one of the most advanced countries in high-tech technology, including electronics, chemistry, pharmaceutical products and the heavy machine-building industry (Baev, *Spying on the West*).

Jordan Baev described the mechanisms and the extent of Soviet espionage in the scientific field: "In the post-war years, the chief of Soviet scientific intelligence was Col. Leonid Romanovich Kvasnikov (1947–64). He was succeeded by Col. Mikhail Ivanovich Lopatin (1964–74) and Gen. Leonid Sergeevich Zaytsev (1975–91). In the early 1960s, the 10th Department of the PGU had seven intelligence orientations: nuclear, aerospace, electronics, medicine, chemistry, new technologies, and information and analyses. The S&T Intelligence officers at KGB representations (*rezidentura*) abroad were codenamed «Line X». After the establishment of Directorate «T» in 1974, the Soviet leadership approved Andropov's proposal to double the staff abroad. Thus, in 1975, the Soviet S&T intelligence services activated 77 of its agents and 42 informers who focused their activity on the US alone, and specifically on 32 principal objects (General Electrics, Boeing, Lockheed, McDonnell-Douglas, Westinghouse, etc). According to a KGB report to the Central Committee of the Communist Party of the Soviet Union (CC CPSU), during the period 1972-7, S&T intelligence obtained about 120,000 pieces of new information with 20,000 schemes and diagrams, which were mainly delivered to the state Defence Industry Committee. In 1979 alone, the Soviet Scientific Intelligence Directorate realized 557 «measures involving operational agents» abroad. In 1980, the KGB delivered more than 14,000 pieces of information and 2,000 models of different technical equipment to various governmental departments and agencies, and to state firms and research institutes. In 1981, it provided 13,500 items and 3,000 models, and in 1982, 10,000 pieces of information and 4,000 models" (Baev, *Spying on the West*).

In his study, Baev highlights the following aspects: starting in 1966, 30 highly trained officers were enrolled in the Bulgarian espionage, some of them completed their PhD in exact sciences or humanities, 20 of them "were sent for one year to the KGB PGU Special School near Moscow (known as «School No. 101»)"; starting in 1971, the information exchange between the two services significantly increased, the KDS had sent KGB 161 reports and 5.6%

of them were deemed as valuable. "According to the next long-term agreement for the period 1975–80, collaboration between the two allied secret services in procuring military S&T intelligence included acquiring new information on US Trident nuclear submarines, Minuteman cruise missiles, the B-1 strategic bomber, and other items. As a result, in the period 1976–8, the PGU-KGB's Directorate «T» sent 643 S&T intelligence references to Sofia, 313 of which were military-related. In 1976 and 1977, the Bulgarian Scientific Intelligence Department sent 463 classified references to Moscow, eight of which were assessed as «extremely valuable», 82 as «valuable», and another 174 as «interesting information»" (Baev, *Spying on the West*).

KGB – STASI (collaborations and information exchange against NATO)

The cooperation between the KGB and the Ministry for State Security (**Das Ministerium für Staatssicherheit**-STASI, 1950-1990) in the GDR was mostly concerned with NATO. The success of STASI in the HUMINT field, achieved thanks to the HV.A, was reached at the level of intelligence communities in the WP member states. For example, in the 1980s, HV.A "ranked the highest among the ten clusters of intelligence to be gathered «military policy, military planning and intentions, military potential of NATO, the USA, FRG [Federal Republic of Germany], other main imperialist powers, and the PRC [People's Republic of China]». The second rank included «armament research and production in the USA and other NATO countries, particularly the development and production of new strategic weapons and weapons systems»" (Schaefer, Bernd, "The Warsaw Pact's Intelligence on NATO").

Following the Soviet model, two espionage structures functioned in the GDR: HV A., within STASI, as a counterpart to the PGU, which operated within the KGB and "Aufklärung" (a department within HV A.), which served as a counterpart to GRU and specialized in gathering military intelligence. "Aufklärung" functioned as an independent structure until 1958, when it became subordinate to the HV A, after a series of high-level recruitments performed by the GDR's military espionage service. HV A can thus be synthesized: "HV A. as the civilian branch was commissioned by the Warsaw Pact to target West Berlin, the FRG, and United States and NATO. The intelligence it gathered was presented to the GDR's top political and military leadership. In 1988, for instance, Department IV of the HVA (Military Espionage) directed 74 FRG citizens as its agents, whereas Department XII, in charge of infiltrating NATO and the European Community, had 72 agents at its disposal to penetrate their institutions. Of the eighteen HV A. departments, four were primarily assigned to monitor and infiltrate specific countries and their

institutions: Department I (Federal Republic of Germany/FRG government), II (FRG parties and institutions), XI (USA) and XII (NATO and the European Community)" (Schaefer, Bernd, "The Warsaw Pact's Intelligence on NATO").

KGB – ÁVH (NATO, USA, Canada, the Scandinavian countries)

The working relationship between the KGB and the ÁVH can be described in very favourable terms, especially after the 1956 Revolution. It was mostly concerned with information exchange related to the following topics: NATO, USA, Canada, the Scandinavian countries. Regarding the issue of Transylvania, the two securities and intelligence services repeatedly used misinformation in order to deceive the Western intelligence community.

On a side note, as leader of the Hungarian Socialist Workers' Party (MSzMP), Janos Kádár continually encouraged the frictions between Hungarian and Romanian citizens in Transylvania in order to preserve a level of tension at bilateral level. More precisely, the Hungarian People's Republic was unjustly referring to a lack of support from the Romanian authorities regarding the Hungarian minority, thus expressing their concern for the Hungarians in Transylvania. These practices were forbidden inside the Soviet bloc but they went unnoticed due to well-organized disinformation campaigns. This type of operations became very successful. For example, a 1964 National Intelligence Estimate (NIE) bulletin incorrectly mentioned growing tensions between the Hungarian People's Republic and the Socialist Republic of Romania (RSR) on the topic of ethnic Hungarians living in Romania (NIE, July 22nd 1964, no. 12-64, p. 9).

The reform of the Hungarian security and intelligence services under Kádár deserves special interest. Practically, there wasn't any particular structure, ÁVH, as experts call it. Instead, everything was organized under the supervision of the Hungarian Ministry of Interior. For this reason, many experts argue that Hungary was the only WP member state that lacked any security or intelligence services. There is no proof that would indicate instructions from the KGB but declassified reports from the headquarters in Lubyanka (TsKhSD, f. 89, op. 5, d. 3, II, 1-14) fail to mention the Hungarian secret services. This fact might be explained by an intention to prevent any kind of suspicion from Romania, thus turning into a *fait accompli*. Nowadays, these situations can be easily revealed but at that time very few people had access to this type of information, as censorship was part of the daily life.

Budapest's actions in diplomacy and foreign policy were justified by the freedom given under the protection of the USSR. Moscow successfully exploited Budapest under the program of active measures. Hungary became

an important source for disinformation and propaganda after many citizens fled to the Western countries in 1956. The ÁVH used the revolution as an opportunity to infiltrate agents among immigrants, especially in the USA and Canada. On the strength of disinformation and an influential Hungarian community, Hungary built itself a positive image during the Cold War and after 1990 as well, being admitted to NATO and the EU before Romania did. The KGB was also involved in the issue of Hungarian emigrants, having infiltrated 200 agents among them (Corson and Crowley, 1986, pp. 268-270).

The year 1968 offers us a less known detail. Throughout the year, Soviet-Hungarian disinformation created a "halo" for Kádár, painting him as an opponent to Moscow and the Warsaw Pact. CIA became the "victim" of this disinformation operation by believing that Hungary shared Romania's position on the issue of interference in Czechoslovakia's domestic affairs (CIA, *Intelligence Memorandum,* May 19th 1968, p. 2).

Kádár's image as a "dissident" and opponent of the Soviet Union lasted long after 1968. This was made possible with the support of the KGB and the Hungarian communities in the USA, Canada and Great Britain. In this regard, Kádár gained a moral advantage that allowed him to promote his agenda on the issue of the Hungarian minority in Romania.

In the early 1970s Kádár was a strong supporter of the so-called "New Economic Mechanism" (NEM), an initiative backed up by all the general secretaries of the CPUS up until Gorbachev (CIA – *Special Analysis,* May 22nd 1982, pp. 10-12). Hungary's intelligence activities benefitted from Soviet human and material support. If Budapest was facing any difficulties, Moscow was ready to act as a tutor by providing intelligence assistance. Kádár's credibility in the West was built upon the support given by the PGU, especially in Finland and France. Both countries made it possible for Hungary to build its positive image in liberal countries. At that time, Kekkonen, later identified as a KGB agent, was the leader of Finland, while left-wing political influences and a stronger support of Moscow became commonplace in France.

KGB – SB (Vatican, USA)

Polish historian Andrzej Paczkowski described the relations between the USSR and the Polish People's Republic (PRL) as follows: "For the purpose of this text I describe Poland's relations with the Soviet Union as that of a vassal. The sovereign power, the Soviet Union, deployed the services of the vassal, Poland, and was obligated to take care of the latter's security in return. Both sides benefited from the arrangement: the vassal enjoyed security and the sovereign thrived off its power. In the case of the vassal, the crux of the

matter concerned not only external security (international relations) but also internal threats (protection against a revolution or a coup), which the vassal could not overcome on its own (as in East Germany in 1953)" (Paczkowski, 2002, p. 4). Starting from this assumption and keeping in mind that the state plays some essential roles (self-preservation, innate sovereignty), we consider that military institutions tend to mimic the particularities of the societies and countries they serve (Toqueville, 2004, pp. 761-767), while the same principle also applies to intelligence/counterintelligence institutions.

The partnership between the KGB and the SB became more and more active in the beginning of the Cold War, "In 1956, during the thaw period, the relations became more – but not entirely – of a partnership. The team of advisers (operating within the Public Security Committee structures) was reorganized into a KGB mission in Warsaw. Still, the chief advisor, Colonel Georgiy Yevdokimenko remained the head of the mission. In January 1957, an official delegation of the Interior Ministry Security Service paid the first visit to Moscow. The agreement that was signed then opened a period of systematic and formalized cooperation of both services, which continued until 1990. The Polish side in the cooperation was mainly represented by the First (intelligence) and Second (counterintelligence) Departments. High level meetings (of the Polish deputy minister and the KGB deputy chairman) were held at least once a year. On 1-3 July 1963, a top level meeting took place in Warsaw with the Soviet delegation led by KGB Chairman Vladimir Y. Semichastny. From May 1961, an official post of the Polish Interior Ministry operated in Moscow" (the «Vistula» Operating Group of the Secret Service) (Bułhak and Paczkowski, 2008, p. 52). The cooperation between the KGB and the SB was mostly related to the religious activity of the Vatican and the USA which was home to an influential Polish community. Regarding the Vatican, the PRL developed an innovation at the level of the SB: "After 1956 operational intelligence gathering against the Vatican was a major task of the MSW. As early as in 1958, ministerial directives stressed the need to gather information on the Vatican's intentions, plans and tactics. A network of agents recruited also among the clergy was to be used to this effect. Passport procedures were used in recruitment. (…)From June 1962, all anti-Church activities were concentrated in Department IV of the Ministry of Internal Affairs, i.e. so-called 4th division of the Security Service (Służba Bezpieczeństwa – SB). It was a specialised unit of the SB, tasked with surveillance, supervision and combating hostile – as they were referred to at that time – activities of the Roman Catholic Church, other religious organisations and associations of laic Catholics. The Department had its provincial branches, namely sections IV of the voivodship headquarters of the

Civic Militia (Milicja Obywatelska – MO). As in other countries in the Eastern Block, in all actions against the Vatican the units of Department IV co-operated closely with Department I of the MSW, i.e. foreign intelligence service of the PRL. This co-operation was regulated by detailed instructions of how to set tasks". (Grajewski, 2008, pp. 178-179)

KGB – StB (NATO, operation ALAN)

After 1948, the activity of CSR's security and intelligence services was hugely influenced by their Soviet counterparts. Following the same model applied in the other member states of the WP, Soviet advisers were appointed to the newly-founded security and intelligence services in the CSR and they imposed themselves due to their previous experience in intelligence/ counterintelligence.

The two security and intelligence services operated under the motto "Struggle for Peace and Socialism" and they used careful planning to synchronize their activities. This particular operation took place once every five years, although initially it was performed annually. "Using their own methods and experience the Soviet KGB advisors begun to define objectives and forms of co-operation to be conducted by Czechoslovak Intelligence, namely by the 1st Directorate (assumed name). Under the concept of the ´Struggle for Peace and Socialism´ the two intelligence services coordinated their activities first on a yearly basis, and later, on the basis of five-year operational plans. The plans referred to the activities conducted by the Centre and by the individual Residencies. The final forms of the operational plans were specified by Moscow after negotiations with the Chief of the Ist Directorate of the Ministry of the Interior (later, the Federal Ministry of Interior). Such a dependent subordinate position required that the activities of Czechoslovak Intelligence were, in practice, conducted against all former capitalist countries around the world. The focus of their activities was to obtain classified documents, resources and secret information of political, military, economic, scientific, technological and state-security-related contents. The operational activity of the intelligence was documented in the agency and operative files". (Bukovszky, 2008, pp. 25-26)

An interesting point in their cooperation, also known as "Operation ALAN", is related to the leaks of NATO classified information in 1982-1986. Otherwise said, "In the fall of the Cold War, at the end of the 1980´s, the American and West German intelligence services discovered and brought to the court a spy group composed of former officers of the US army operating in the territory of the Federal Republic of Germany (FRG). Through their illegal

activities they managed to gravely threaten the security and stability of the North Atlantic Treaty Organisation (NATO) and the United States of America. During its 17 years of operation the group now known as the Clyde Lee Conrad spy group would deliver to the member states of the Warsaw Pact copies of top secret documents of military and strategic contents related to the operational plans, regulations, procedures, tactics and strategy, nuclear armament, and scientific and technological knowledge of the NATO armed forces" (Rendek, 2008, p. 223).

In the Institute for the Study of Totalitarian Regimes of the Czech Republic, "Cooperation in the Eastern Bloc 1948-1989: documents on bilateral cooperation", are available on collaboration between socialist countries' intelligence services. Information exchanges and cooperation between CSR and SRR are reduced to only two documents, unlike the collaboration with GDR, where 102 documents are available. Within the same project in the section dedicated to "International Cooperation in 1989", CSR had collaboration protocols with all services in the Eastern Bloc, especially with KGB., except for the SRR Securitate.

Conclusions

Russia's assertive role in Central and Eastern Europe became very evident after the end of the World War II, when this area entered the hegemonic Soviet sphere. The expansionist tendencies of Medieval Russia/Imperial Russia/the Soviet Union/the Russian Federation can be explained by a strong sense of insecurity, still present nowadays. For Russia, territorial expansion was essential in building a solid state and ensuring its security, and this aspect was featured in the Russian interwar foreign policy. The logic of "conquering" Central and Eastern European states was part of creating the "glacis/security belt", therefore obtaining security through territorial conquests in two stages: 1) 1939-1940 by signing the Ribbentrop-Molotov Pact; 2) 1944-1949 Red Army conquests and deliberate concessions from the Americans and the British.

The active measures, designed by Soviets, still are truly sophisticated instruments for creating strategic events in order to gain short, medium, and long-term advantages in socio-economic, political, military and intelligence terms. The intelligence war, in which the active measures program found plenty of use, was dominated by the Soviet Union and the allies from the Warsaw Pact against NATO and the West.

The hidden war fought by the Soviet Union, either through direct actions or middlemen, was part of a bigger strategy that repeatedly tried to use favoured international political actors (the other Warsaw Pact countries) to verify the power of a potentially hostile power inside the Socialist Bloc and Romania is a relevant example. Nowadays, from a realist perspective, this practice is called **offshore balancing**.

Active measures can be identified in what we call today irregular/ unconventional/asymmetrical/fourth generation warfare. Otherwise said, it is another tradition inherited by the Russian Federation.

References:

1. Arhivele Naţionale Istorice Centrale (ANIC), Collection Tratatul de la Varşovia. Ministerul de Externe, (1954-1991, 1993), file no. 23/1966.

2. Andrew, Christopher, Mitrokhin, Vasili, (2001), *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*, SUA, Basic Books.

3. Andrew, Christopher, Gordievski, Oleg, (1994), *KGB: istoria secretă a operaţiunilor sale externe de la Lenin la Gorbaciov*, translated by Doina Mihalcea – Ştiucă, Bucharest, Ed. All.

4. Baev, Jordan, (2008), „MGB/KGB Cooperation with the Bulgarian Intelligence & Security Services 1944-1989" in *NKVD/KGB Activities and its Cooperation with other Secret Services in Central and Eastern Europe 1945-1989*, part II, Prague, November 19-21.

5. Barron, John, (1983), KGB Today: *The Hidden Hand*, New York, Reader's Digest Press.

6. Belügyminisztérium, (1969), *A Magyar Népköztársaság belügyminiszterének 0010. Számú PARANCSA*, 10-21/10/1969, Budapest.

7. Bittman, Ladislav, (1972), *The Deception Game: Czechoslovak Intelligence in the Soviet Political Warfare*, Siracusa, Syracuse University Research Corporation.

8. Idem, (1985), *The KGB and the Soviet Disinformation: an Insider's View*, Washington, Pergamon – Brassey's.

9. Bułhak, Władysław, Paczkowski, Andrzej, (2008), „Relations between the Soviet and Polish Security Services in 1944–1990" in *NKVD/KGB Activities and its Cooperation with other Secret Services in Central and Eastern Europe 1945-1989*, part II, Prague, November 19-21.

10. Bukovszky, Ladislav, (2008), „The Archive of the Nation´s Memory Institute in the Capacity of Resources for KGB Activities" in *The NKVD/KGB Activities and its Cooperation with other Secret Services in Central and Eastern Europe 1945-1989. Anthology of the international conference*, Alexandra Grúňová (ed.), Bratislava. 14-16 November, 2007, Nation's Memory Institute.

11. Carnegie Middle East Centre, (2010), *The Military Doctrine of the Russian Federation*, translated and approved by Russian Federation presidential edict on 5 February 2010.

12. CIA, (May 19, 1968), *Intelligence Memorandum: The Situation in Czechoslovakia as of AM EDT*, declassified on October 17th 2002.

13. CIA, (May 22, 1982), *Special Analysis, USSR – Hungary: Interest in the Hungarian Example*, declassified on January 29th 2001.

14. Clizbe, Kent, (1999), *Willing Accomplices: How KGB Convert Influence Agents Created Political Correctness, Obama's Hate – America - First Political Platform, and Destroyed America*, SUA, Andemnca Publishing.

15. Corson, William R., Crowley, Robert T., (1986), *The New KGB: Engine of The Soviet Power*, New York, William Morrow.

16. Dungaciu, Dan, (coord.), (2017), *Enciclopedia relațiilor internaționale*, vol. II N-Z, Bucharest, RAO Distribuție.

17. Duroselle, Jean – Baptiste, (2006), *Istoria relațiilor internaționale 1919-1947*, vol. I, translated by Anca Airinei, Bucharest, Ed. Ştiinţelor Sociale şi Politice.

18. Dziak, John J., (1987), *Chekisty: a history of the KGB*, SUA, Lexington Books.

19. Hingley, Ronald, *The Russian Secret Police: Muscovite, Imperial Russian, and Soviet Political Security Operations*, New York, Simon and Schuster.

20. Enciclopedia Britanica, available at: http://www.britannica.com/EBchecked/topic/426484/Okhranka#275729.hook.

21. Eszter, Tóth, (2011), „A politikai hírszerzés szervezettörténeti vázlata, 1945–1990", in *Betekintő*, 2011/2, Budapest.

22. Gábor, Tabajdi, (2013), *A III/III krónikája*, Budapest, Jaffra.

23. Fodor, Neil, (1994), *The Warsaw Treaty Organization. A political and Organizational Analysis*, USA, Palgrave Macmillan.

24. Grajewski, Andrzej, (2008), „Security Services of the Polish People's Republic against the Vatican in 1956-1978" in *The NKVD/KGB Activities and its Cooperation with other Secret Services in Central and Eastern Europe 1945-1989. Anthology of the international conference*, Alexandra Grúňová (ed.), Bratislava, 14-16 November 2007, Nation's Memory Institute.

25. Gunn, Jeremy T., (2009), *Spiritual weapons: the Cold War and the forging of an American national religion*, Under the auspices of the Leonard E. Greenberg Centre for the Study of Religion in Public Life, Trinity College, Hartfort, Praeger.

26. Hoffman, Frank G., (2009), „Conflict in the 21th Century: The Rise of Hybrid Wars", in *National Defence University, Institute for National Strategic Studies*, Washington DC.

27. Kalugin, Oleg, (January 1998), „Inside the KGB: An interview with retired KGB Maj. Gen. Oleg Kalugin," CNN, available at http://www3.cnn.com/SPECIALS/cold.war/episodes/21/interviews/kalugin.

28. Keating, Kenneth C., (1981), *Maskirovka: The Soviet System of Camouflage*, Germany, U.S. Army Russian Institute, Garmisch.

29. Knight, Amy W., (1990), *The KGB: Police and Politics in the Soviet Union*, Boston, Unwin Hyman.

30. Lasota, Marek, (2003), „O Raporcie Sejmowej Komisji Poświęconym Samodzielnej Grupie „D" w MSW. Informacja o Działalności Komórek „D" Pionu IV Byłej Służby Bezpieczeństwa", in Instytutu Pamięci Narodowej, Nr. 1 (2004), Styczeń.

31. Lind, William S., (September – October 2004), „Understanding Fourth Generation War" in *Military Review*.

32. Lippman, Walter, (1947), *The Cold War. A study in U.S. Foreign Policy*, New York.

33. Mattis, James N., Hoffman, Frank G., (November 2005), „Future Warfare: The Rise of Hybrid War", in *U.S. Naval Institute (USNI)*, Proceedings Magazine, vol. 132/11/1,233.

34. Mitrokhin, Vasili, (2004), *KGB Lexicon: the Soviet intelligence officer's handbook*, London, Routledge.

35. Mitrokhin, Vasili, Andrew, Christopher, (2003), *Arhiva Mitrokhin: KGB în Europa şi în Vest*, translated by Ion Aramă, Bucharest, Ed. Orizonturi.

36. Idem, (2006), *Arhiva Mitrokhin: KGB-ul în lume*, vol. II, translated by Anca Irimia Ionescu, Bucureşti, Ed. Orizonturi.

37. Monas, Sidney, (1961), *The Third Section: Police and Society in Russia under Nicholas I*, Cambridge, Harvard University Press.

38. Münkel, Daniela, (ed.), (2015), *State Security. A reader of the GDR Secret Police*, Berlin.

39. NIE, *Changing Patterns in Eastern Europe*, July 22nd 1964, no. 12-64, declassified on July 16th 1993.

40. Olaru, Stejărel, Herbstritt, Georg, (2005), *Stasi şi Securitatea*, translated by Viorel Buta şi Mihai Alecu, Bucharest, Ed. Humanitas.

41. Paczkowski, Andrzej, (2002), *Polish – Soviet Relations 1944-1989: The Limits of Autonomy*, Institute of Political Studies, Warsaw.

42. Persak, Krzysztof, Kamiński, Łukasz (eds.), (2005), *A Handbook of the Communist Security Apparatus in East Central Europe: 1944-1989*, Warsaw, Institute of National Remembrance.

43. Pleskot, Patryk, (2016), *Kill. Political assassinations in the PRL*, Krakow, Znak Horyzont Publishing House.

44. Pirnie, Bruce R., (1985), *Soviet Deception Operations in World War II*, Washington D.C., U.S. Army Center of Military History.

45. Pringle, Robert W., (2006), *Historical Dictionaires of Intelligence and Counterintelligence Series*, SUA.

46. Rendek, Peter, (2008), „Operation ALAN – Mutual Cooperation of the Czechoslovak Intelligence Service and the Soviet KGB as Given in One of the Largest Leakage Cases of NATO Security Data in the Years 1982 – 1986" in *The NKVD/KGB Activities and its Cooperation with other Secret Services in Central and Eastern Europe 1945-1989. Anthology of the international conference*, Alexandra Grúňová (editor), Bratislava. 14-16 noiembrie 2007, Nation's Memory Institute.

47. Robinson, Paul, (2010), *Dicționar de securitate internațională*, translated by Monica Neamț, Cluj – Napoca, CA Publishing.

48. Sawa – Czajka, Elżbieta, (2014), „Rebel – war in Ukraine" in *The Journal of Kolegium Jagiellonskie Torunska Szkola Wyzsza*, vol. I: 25-31.

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

50. Schaefer, Bernd, „The Warsaw Pact's Intelligence on NATO: East German Military Espionage against de West" in *PHP*.

51. Shultz, Richard H., Godson, Roy, (1984), *Dezinformatsia: Active Measures in Soviet Strategy, Washington DC*, Pergamon – Brassey's.

52. The Congress of the USA, (1982), *Hearing Before the Permanent Select Committee on Intelligence on Soviet Active Measures, 97th Congress*, second session, July 13 and 14.

53. TsKhSD, f. 89, op. 5, d. 3., II, 1-14, „Raportul Anual al KGB, 1967", 06.05.1968, in *Cold War International History Project (CWIHP)*.

54. Toqueville, Alexis de, (2004), *Democracy in America*, vol. II, translated by Arthur Goldhammer, New York.

55. United States Government Accountability Office (U.S. GAO), (2010), *Hybrid Warfare. Briefing to the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services, House of Representatives,* September 10.

56. Volkoff, Vladimir, (2000), *Dezinformarea armă de război*, translated by Andreea Năstase, Bucharest, Ed. Inciatus.

57. Watts, Larry L., (2011), *Ferește-mă, Doamne, de prieteni ... . Războiul clandestin al Blocului Sovietic cu România*, translated by Camelia Diaconescu. Bucharest, Ed. RAO.

58. Wiedmann, Roland (coord.), (1996), *Die Organisationsstruktur des Ministerium für Staatssicherheit 1989,* Berlin, Ed. BstU.

59. Wolf, Markus, McElvoy, Anne, (1998), *Memoirs of a Spymaster. The Man who Waged a Secret War Against the West,* Pimlico.

THE INDUSTRIAL ESPIONAGE, A STRATEGIC OBJECTIVE OF THE ROMANIAN COMMUNIST SYSTEM BETWEEN 1965 AND 1989

Iulia Cristina SACALAŞ*

Abstract

During the Cold War, in the shadow of ideological confrontation, the attention of the academic literature on the small and medium countries within the confronted blocs was limited. This paper aims to redress, to a certain extent, the imbalance created by the significant amount of attention received by the great powers in the historiographical debate of the Cold War in comparison to other countries.

Given the significant role and importance secret services and their labour had in the development of the ideological war, countries with relevant endeavours in this matter are worth a more careful attention. The activities of the Romanian secret services were well connected to the aims established by the communist system while using interesting methods and techniques. Analysing some of these would enrich significantly the historiographical collection of the Cold War.

This paper is part of a study that aims to fill in a niche by trying to find out whether industrial espionage was a strategic aim for the second and last part of the Romanian communist system, namely between 1965 and 1989. This paper also highlights the contribution made by the Romanian secret services to the course and development of the Cold War and tries to give a specific and specialised context for the nowadays democratic Romania. The examination of the methods used by the Romanian secret services in connection to the established objectives gives a general perspective of the aims of the Romanian communist system during the Cold War and reveals the importance industrial espionage had on it.

The limited resources available might interfere in the quality of the analysed research. However, it leaves an open door for further investigation that might eventually answer some of the questions rose in this paper.

Keywords: *industrial, espionage, Communism, Ceausescu, secret, Caraman.*

* MA Intelligence and International Security, King's College London, iulia.sacalas@gmail.com

Introduction and brief literature review

This study is of particular relevance for this panel and provides an unusual perspective on what were the impacts of industrial espionage in a particular context. The industrial espionage that Romanians pursued so fervently in the second part of the communist era marked the country for future decades and its position within the international stage. The phenomenon seems to be a recurring pattern.

In the context of an aggressive capitalist system, paradoxically, industrial espionage has become again a topic of interest. Mainly conducted by major corporations, their link to their country of origin is important for the shaping of the international dynamics at economic and political level. The Romanian example, although in a different context, where the system was limited and shaped by the values of socialism and the example of the USSR, helps to create the framework of what industrial espionage means, brings and aims in different contexts.

The ideological clash represented by the Cold War was transformed into an authentic conflict that, as the Romanian historian Cristian Troncotă would say, although apparently cold, in fact as hot on the secret scene as to impact each of the historical events of the era (Troncota, 2006, p. 5).

With the study of secret intelligence of this period, historians understood, at least partially, what the Cold War was about. More importantly, they understood the relevance and the weight intelligence and secret actions gained meanwhile. Therefore, they described the Cold War as an intelligence conflict where the fastest and brightest in handling information while getting under the opponent's skin was the one to be victorious. Both sides tried to focus on this matter, creating complex structures of intelligence and adapting the old ones to the new international political and economic reality. They used espionage as main offensive weapon and counterintelligence as a defence tool.

Regardless the similar ideologies from within each bloc, among their members there were some countries that aspired to be more relevant and to have a different position in the international system, trying to break freer from under the socialism or liberalism umbrella. One of these countries was Romania who, even though rarely mentioned in the international historical analysis of the Second World War, played an important role in ending it sooner (Troncota, 2006, p. 6).

Through these ambitions, the Cold War, with its information and arms race, was seen by the Romanians as a good opportunity to weaken the strong link and control the Soviet Union had established on their country after the world war. To achieve this, Romania established specific objectives and

worked strategically and thoroughly towards this position, relying strongly on intelligence and espionage. They invested so much in their intelligence system that it affected the social one they were trying to defend and develop in appearance, leading to a Revolution in the winter of 1989 and eventually to its disappearance.

The historiography of the final decade of the twentieth century and furthermore, of the twenty first century, has not paid attention to the Romanian activities during this period or on its interesting political and economic dynamics. Even locally, few Romanian historians and political scientists have researched and analysed this period with the actions that entailed and the impact that these had on the Romanian society and its development during the Cold War and after it. Most of the Romanian historiography is dedicated to the study of the communist system installed after the Second World War, the dissidence it involved, its dictators and the development of the relations with the Soviet Union as an important pillar of the communist system.

Relying on the previous research of the communist system in Romania, of the functioning of its secret services, of the objectives developed by the communist leaders during the Cold War and of the development of the relations with the Soviet Union, this paper is trying to understand if the industrial espionage was a strategic objective of the Romanian communist system between 1965 and 1989.

The importance Romania had during the Cold War is becoming more interesting for the historiography nowadays and could turn out to be noteworthy in explaining and understanding missing perspectives of this period.

The historiography of Cold War Romania has not been able to develop fully the potential explanations and analysis regarding methods used by the Romanian secret services or their role during this time. The institution of *Securitate*, the main body of the Romanian security service during the communist era, was widely studied along with its relationship with the communist system. However, some of the deep analysis of its true importance is missing due to lack of access to relevant primary sources. Some historians focused their attention on the development of the Romanian communist system and of its activities in relation to its aims as a first step in introducing the role Romania played in the "behind the scenes" war between the two blocs.

Dennis Deletant, Cristian Troncota and Pierre Accoce (with Daniel Pouget) were among the most important historians to develop some insights related to the institution of *Securitate*. The three of them focused their studies on different aspects related to the Romanian secret services and their

development within the communist system. While Deletant and Troncota direct their attention on the historiography of the insitution, Accoce and Pouget are more interested in some specific methods Romanians used to achieve their objectives.

The historian Cristian Troncota analysed in various detailed studies the relations between Romania and the Soviet Union and the role played by the Romanian secret services in the development of these relations. According to him, the development of the *Securitate* was strongly influenced by the actions the Soviet Union was taking towards Romania. The country was deeply penetrated by the Soviet secret services. It was considered by them one of the most problematic countries, able to disturb the Soviet influence over the Eastern bloc and already aiming at it. This comes strongly related to the political and economic aims of the Romanians, established by the communist leaders.

Dennis Deletant, also a reference in the study of the Eastern European bloc and the Romanian system particularly, focuses his research in how the security intelligence system had developed during the Cold War. Even if he explains the evolution of the Romanian security intelligence services, Deletant does not focus his area of expertise on the specific methods the *Securitate* used in order to achieve the aims established by the communist leaders. Deletant managed to study some of the files of the *Securitate* and explained along his studies the importance this institution had in the development and maintenance of the communist system. In order to detect and analyse its importance, he gives a thorough explanation of the structure of the institution and the changes within it as well as its actions and how they affected the society and the system. He talks about the ´legacy´ the institution left on Romania and how this legacy affected the transition to democracy from 1989 to 1991 and its further evolution from 1991. According to Deletant, Romania "shared with all the communist regimes of Eastern Europe a total reliance upon terror as an instrument of political power" (Deletant, 2001, p. 159).

As Deletant's analysis concludes, following the aim of achieving a certain independence from the USSR was especially difficult during the leadership of Gheorghiu-Dej, whose institutions were deeply penetrated and controlled by the Soviets. However, this situation changed as ´Khrushchev's removal on the 14 October 1964 as Soviet leader [that] offered Gheorghiu-Dej a further chance to consolidate his break with Moscow´. The leader took the opportunity and the next Soviet ruler, Leonid Brezhnev finally acceded to retire the Soviet counsellors from Bucharest. Despite this, one of the starting points of this research is related to the fact that in spite of the retirement of the counsellors from Romania, the institutions remained deeply penetrated by Soviet spies. A thorough analysis of the context and actions taken by the Romanians indicates

that the strategic elements of the Romanian domestic and foreign policies were strongly influenced by this aspect. The continuous presence of Soviet officials within the Romanian apparatus was, probably, one of the aspects that pushed the communist leadership to establish the full independence of the Romanians from Soviet influence as main national objective, and the intelligence services as a main tool in achieving it. Industrialisation was going to be a key aspect in achieving this national objective.

Another author of relevance for this paper and the topic surrounding it, Pierre Accoce, focused his study of the Caraman network in explaining how the industrial espionage was developed, also by giving a brief perspective of the motivations. However, Accoce´s story of the Caraman network does not provide an extensive explanation of the strategic nature of the actions of the network of Mihai Caraman or their level of contribution to the industrial conglomerate.

This study, relying particularly on the work of these historians, is aiming to provide a general understanding of the strategic nature of the industrial espionage practiced by the Romanians during the second period of the communist era and after the instalment of Nicolae Ceausescu at Cotroceni, the residence of the country's leader. As the topic studied is of recent interest amongst historians, the paper relies on the qualitative method of reviewing the existent literature and the study of primary sources related to the main topic of interest, available through the Romanian National Archives of the *Securitate*. It also includes a brief study case, relevant in answering the question raised by it.

The institution of Securitate in the Cold War Romania

According to several historians, the first period of the communist system was marked by repression and the elimination of the opposition. Defined by the Soviet model of dictatorship, the communist system was installed in Romania following closely the steps of the Soviet model of repression and terror. The main instrument used to achieve such measures was the *Securitate*. Mass arrests and a general sentiment of fear was what made Gheorghe Gheorghiu-Dej's (the first long term communist leader after the Second World War) system comparable to George Orwell's dystopia of *1984*. Of course, many questions regarding this system were left unanswered.

With the death of Gheorghiu-Dej, repression was no longer the main purpose of the communist system. With a much more developed communist rule, the new General Secretary of the Romanian Communist Party and leader of the country, Nicolae Ceausescu, started to focus more on the breakaway of

the Romanian nation from the Soviet overlord rather than continuing the terror system of his predecessor. Even so, the historiography of the Romanian communism refers to this period as the period marked by the ignominy of human dignity and human rights. Despite this description and according to conclusions drawn by Dennis Deletant, Ceausescu´s system "never used the tactics of mass arrests and internal deportations that were a feature of most of the Dej era" (Deletant, 2001, p. 159).

Therefore, Nicolae Ceausescu focused the Romanian state policy much more on the aim of breaking-up with the Soviet Union than Gheorghiu-Dej had the chance to. With Ceausescu's coming into power, the *Securitate* had to be reformed completely once the Constitution was enhanced; Romania was transformed into a Socialist Republic from a People´s Republic.

The External Intelligence Department

According to the Romanian historian Florian Banu, the creation of the External Information Direction was one of the most important moments of the history of the Romanian secret services during the communist era (Banu, p. 102).

From the beginning of the communist rule in Romania, espionage started to be an important element of the secret services, especially given the historical context of Cold War. Espionage activities were under the command of the *Special Intelligence Service*. After the replacement of the Special Intelligence Service by the *General Directory of the People's Security*, the external intelligence activities started to be undertaken by the *Direction A – External Intelligence of the General Directory of the People´s Security*.

With the merger of the Ministry of State Security with the Ministry of Internal Affairs, was created the Department of External Intelligence (*Departamentul I Informatii Externe – DIE*). The external intelligence ran under this name until 1963, when it was renamed the General Direction of Intelligence (*Directia Generala de Informatii – DGI*). Latter, in 1968, DGI became the General Direction of External Intelligence (*Directia Generala de Informatii Externe – DGIE*).

In spite of all the changes in the denomination of the institution, its structure remained more or less the same, including three more directions: the 5th Direction, in charge of the scientific and technical espionage, the 6th Direction, in charge of the *illegals* and the 7th Direction, in charge of the infiltrations in the foreign intelligence, counterintelligence services and the defence counterintelligence of the representatives of the state as well as the fight against the resistance movement and reactionary emigration. (Banu, p. 3)

With the passing of the Council of State Security under the jurisdiction of the Ministry of Internal Affairs, there were some changes in the structure of the *DIE*. Only after a year of this merger, the activity of the department was regulated.

The defection of general Ioan Mihai Pacepa[1] in July 1978, left an important mark on the Romanian communist system at the time, as well as some historiographical memoirs that contributed to the general analysis of the Romanian secret services during the communist era. Pacepa related in one of his publications how the *DIE* functioned after its merger with the Ministry of Internal Affairs. According to him, he and the general Nicolae Doicaru[2] pushed a proposal to Ceausescu to legalise the activity of the Department without publishing the regulation. This, according to Pacepa, was much needed as the Department was acting illegally in many aspects of its activity, as most of its activities were contradictory to the Constitution.

The decree was going to contradict the Constitution anyways but, to get it signed by the leader, Pacepa and Doicaru had to collaborate with Gheorghe Oprea, Ceausescu's vice-Prime-Minister and counsellor. To redact the decree in such fashion so the dictator would sign it, the generals mobilised the most important individuals within *DIE*, including General Mihai Caraman, an important and respected figure within the service, given his achievements (some outlined later in the paper). On 23 June 1973 the dictator signed the *Decretul Consiliului de Stat, nr. 363* (the Decree of the State Council number 363) regarding the organization and functioning of the Department of External Intelligence. The document was not published in the Romanian Official Gazette (*Buletinul Oficial*) and it was made available only to the specialised structure of the Ministry of Internal Affairs (Banu, p. 6).

According to Pacepa, this decree created the mafia of espionage of Ceausescu, and as such, remained one of the most secret documents of the history of Communist Romania. It is worth having a critical perspective on Pacepa's view, as he had also mentioned that he had a great stake in the promotion and creation of the decree. Thus, his indignation and criticism when relating the masking of the activities of the department under cultural, diplomatic and religious activities should arouse a certain degree of reluctance. In the Department, the external espionage activities were under the diplomatic umbrella since 1941.

With this decree, the Romanian external intelligence started to have a specific and characteristic structure, until 1978, although it did not change significantly from the previous one. It also benefited of modernisation of some

[1] Former general of Communist Romania, who defected to the United States in July 1978.
[2] General within *Securitate* and chief of DIE from 1959 to 1978.

of the methods and means used by the Romanian espionage. All the informers were conspired officers that worked aiming to eliminate any Soviet (and probably Western) threat as well as to develop Romania´s possibilities to become fully independent from the Soviets. Historian Florian Banu gives a detailed explanation of how the department worked including the financial retributions and other types of incentives the service used to maintain its informers loyal. Banu criticises Pacepa's perspective and explains that the acknowledgement of the system by the Western intelligence services discredited the professionalism and the correct functioning of such a complex structure put together and reformed in so many occasions. The fact that Western services were aware of the Romanian external intelligence organisation was discovered by Mihai Caraman through one of his agents in Austria that was able to obtain a document in which the organisation and functioning of *DIE* was described minutely. Regardless, the decree had lost any value after the defection of Pacepa, one of its promoters. The entire system had to be modified and the time lost by doing it had important consequences on the communist system.

After Pacepa's defection and Doicaru's replacement in 1978, as a result of Pacepa's defection, the department was renamed the Centre of Foreign Intelligence (*Centrul de Informatii Externe – CIE*), having slightly different of a structure and organisation. The institution was organised focusing its activities on regions and specific espionage objectives. However, Romanian espionage suffered irreparable damages under Nicolae Plesita, its new leader, and the external espionage stopped being a major matter of interest.

Numerous other defections were encouraged by Pacepa´s. The communist system started being in crisis and the secret service had to focus on preventing further defections and trying to repair the damage made by the previous ones on the country´s reputation. The service focused on unsuccessful counterintelligence activities and on restoring the reputation of the secret services and the Romanian communist system both domestically, among its citizens, and abroad. In consequence, the industrial espionage ceased from being among the strengths or main objectives of the Romanian external intelligence activities.

The industrial espionage from the perspective of the general Ion Mihai Pacepa

Nicolae Ceausescu might have seen a very good opportunity to be the beloved leader of the Romanians, by establishing Gheorghiu-Dej´s policy of independence as the cornerstone of the communist system under his rule.

This policy and the personality cult have worked together for Ceausescu's regime, helping him, supposedly, to achieve the supreme leadership of the country. Regardless, during the era of his rule, the secret services were used as the most important tool to succeed in achieving the independence from Soviet umbrella. The most solicited department of *Securitate* on this matter was the Department of External Intelligence (*DIE*).

According to general Ioan Mihai Pacepa, Ceausescu based the entire economy of the country on the industrial espionage. The former *Securitate* general reveals in his memoirs important intelligence sources the Romanians had obtained from the West. Later declarations of Pacepa stated that according to Ceausescu, stealing from the West was moral, cheaper (than investing in research) but of great effort, and the information gathered with such efforts by *DIE* had to be used smartly in developing the country's industrial arm.

In 1967, the leader used some of the information already gathered from abroad to attract representatives of the Western countries to Romania. He transmitted them that Romania intended to import one of the most important chemical businesses from the West. Companies from England, West Germany and Italy came to Romania with large amounts of general documentation on the polystyrene industry. One French company though, came with an important concrete technical project, already put in practice in other Western countries. Even though the representatives of the company had their documentation well secured during the night, the Romanian espionage managed to obtain the documents that were photographed in detail. After obtaining the useful information, the Romanian government retracted its importation interests. Furthermore, Ceausescu ordered Mihai Florescu, the Minister of the Chemical Industry at the time, to put together a budget on the implementation of the project stolen from the French. The idea and plan of the project were attributed to Ceausescu's wife, Elena, who was known as being a chemist, praising ´her idea´ that had brought the country a USD 15 million contribution to the economy. In eight years, the project was finalised, and the leader opened what he called ´the diamond of the petrochemical industry´, a polystyrene fabric. The complex, constructed in Borzesti, became an important reference point of the Romanian industry. After such a success of the industrial espionage, Ceausescu gave more importance to this practice for the Romanians as a society and as country in the active process of industrialisation. However, according to Pacepa, Ceausescu used industrial espionage to fulfil his megalomania dreams only. These perspectives are always subject to questioning as they rely on subjective perspectives.

Furthermore, Ceausescu followed closely the actions of the Soviets in all the areas of the industrialisation. In 1970, Romania and the USSR signed a friendship treaty at Bucharest, on which occasion Ceausescu received important information related to the espionage activities conducted by the Soviets from the Soviet Prime Minister, Aleksei Kosighin. This concluded in the Decree 272 that raised the espionage activities to the rank of state policy.

In 1972, Ceausescu found out from the Bulgarian president, Todor Jikov, that all the large tonnage vehicles used to transport to the West fruits and vegetables were controlled by the state's secret services. Therefore, the dictator ordered all the Romanian International Transportation vehicles (TIR) to be passed under *DIE*'s supervision. The chauffeurs of the vehicles were replaced by intelligence officers and the Romanian external intelligence managed to counterfeit all the Western custom seals. They were further used to reseal the vehicles, so they would not be controlled at the border and therefore be able to carry secret intelligence in all its forms. They managed to traffic high amounts of illegal drugs and arms. No records of the amounts trafficked through this method were found, including through research of the Romanian National Archives.

Most of the information provided by the Soviets was used in a clever manner by Ceausescu. He transformed the Romanian Civil Air Fleet, TAROM, in an undercover espionage organisation. It was used both for intelligence purposes, carrying diplomatic intelligence and human and equipment trafficking. The management as well as the cabin crews and the international representatives of the company were intelligence agents from *DIE*. The same happened with Navrom, the Romanian Agency of Naval Transport, that in 1975 was passed under the jurisdiction of *DIE* at the suggestion of Yuri Andropov, the chief of KGB. Shortly after, the external intelligence started to use the naval service to import illegally industrial and military equipment (tanks from Israel and radar installations from England and Italy etc.).

Ceausescu also found out about the intention of the Soviets to create ´mixed societies´ with the Western companies. He stole this idea and, after signing a secret decree, ´so secret that it was handwritten´, as Pacepa related, he put the latter in charge of them. The mixed societies had industrial and technological espionage purposes. The internal regulation of these societies specified that the employees in management positions had to collaborate with the secret service. Again, *DIE* oversaw them and their functioning. These societies had as sole contribution the intelligence gathered, as on economic level they failed massively. One of the examples cited by Pacepa was the automobile company, Oltcit that collaborated with the French one, Citroen. The final purpose of this collaboration, from the Romanian perspective, was

the collection of a large amount of intelligence that would have allowed the Romanian production, based on French ideas, to export a significant number of automobiles to all the external markets, boosting the economy of the country. However, the focus of the employees was directed merely to the espionage activity. Twelve years after its creation, it went bankrupt, having produced by 1990 only 1.5% of the initial planned production (Pacepa, 2013, p. 213).

The conclusion that can be withdrawn by analysing this information, that Ceausescu was eager to transform every commercial service into a secret service supplier of large amounts of intelligence, supports the argument of this study. Spying and stealing information from any reachable party, including the Soviet overlord, without considering potential consequences of the undertaken actions, proves the strategic importance and the extent of the industrial espionage, despite the limited sources of intelligence to support it. It also gives a brief perspective of the levels on which the Romanian secret services collaborated with the Soviet ones.

As stated previously, it is important to analyse critically the information given by Pacepa as he criticised a system encouraged by him prior to his defection. Additionally, his insights are not backed by any public primary sources that can prove the objectiveness of his statements. A general line of judgement can be traced and even though the information might have suffered intended inaccuracies, the fact that Ceausescu put industrial espionage on a leading place is obvious. If it did it for personal or patriotic aims remains questionable as the answer can only be the result of a speculation. It gives space to further research, nonetheless.

The Caraman network – insights of the Romanian espionage methods

Nicolae Ceausescu inherited, as part of the development of the policy of independence, a very important and useful element of the secret services, the Caraman network, among the most important espionage weapons Romania had. The network was tediously-built by Mihai Caraman with the aim of providing a tool useful enough to distract the Soviets from the Romanian ambitions and from the gradual elimination of the Soviet agents from the Romanian institutions. The network aimed at providing important intelligence for achieving the ultimate objective of an independent country. Mihai Caraman was general of the *Securitate* with an extended experience in the Ministry of Internal Affairs and the Romanian Communist Party. He worked at the

External Intelligence Department (*DIE*) within the Service France-Benelux-Italy, under diplomatic cover.

The network divided its activity in two parts: from the fifties until 1964, when Ceausescu came to power, and after 1964 until 1989 when, allegedly, Ceausescu took more explicit actions in breaking up with the USSR. However, the network started its activity, fully subordinated to the party's desire of achieving independence, in 1960, when Gheorghiu-Dej began to instil the possibility of an independent country. From 1961 until 1969, Caraman managed one of the most powerful and efficient espionage networks among the communist countries that created significant damage to the Western defence and economic organisations. In this period, Caraman obtained a very large number of documents from his spies, who were working mainly at NATO.

With the creation of NATO, the Soviet espionage gave special attention to the organisation. Such was the case that NATO was the victim of Soviet related espionage every year, as the defence measures taken by the Member States did not seem to have a useful effect. However, given the strict supervision of the Soviets on their own territory, the Western espionage in the East had to rely on defections rather than infiltrations. This is also how the Caraman network was dismantled. Pierre Accoce described the Western measures of defence as inefficient, however, good enough to attract useful agents with a great amount of information from the East. This suggests that the Cold War might have been won by the Soviet bloc if the secret services had had a better acceptance within the populations of its countries.

Some months after the comeback to power of General Charles de Gaulle in France, Mihai Caraman was relocated to Paris at the Romanian commercial representation. The choice of this historical context (the Cold War) to create such a complex network of espionage, shows that the Romanians knew how to take advantage of the situation. The final half of the 50s and furthermore, the 60s, hosted a wide range of events that kept the main rivals of the Cold War, especially the Western countries, tense and vigilant. Caught in the middle of the Algerian war of independence, France could not react as fast and efficient to both internal and external threats. Also, the controversial Cuban Missile Crisis, the assassination of John F. Kennedy, the Prague Spring and its conclusion into the invasion of Czechoslovakia in August 1968, were distractions that gave Romania a good opportunity to react silently and efficiently within the secret war.

Caraman had under his command 12 handlers in charge of controlling the informers, some of whom were controlled directly by him. He appointed them among the Romanian diplomats, and thus none could have been arrested because of the immunity gave by their diplomatic status. According to the later

disclosures of the defector Ion Iacobescu, member of the network, the Caraman network was formed by: Mihail Simula and Ion Paduraru, working at UNESCO, Mihail Georgescu, Gheorghe Ionescu, Eugen Visan, Pavel Cismaru, Constantin Mirea, Marin Negrea and Mihai Ilie working at the Romanian Embassy in Paris (Accoce, 1999, p. 102).

Caraman analysed thoroughly every target and managed to lead the way of his handlers to the manipulation of these individuals and of many others. At first, he patiently observed them by creating their profile, studying their weaknesses and building up the strategy to manipulate them. He then attracted them, manipulated them and finally blackmailed them to achieve his goals.

The particularity of the Caraman network is marked by the fact that it managed to create a varied network of spies that were controlled through a variety of methods and that provided a great amount of different types of intelligence. Even though we are referring to the industrial espionage as a strategic objective of the communist system, it is worth mentioning that the damage that this network made was referred to important industrial, economic and scientific intelligence. This network was probably one of the most important tools of the communist system in obtaining industrial espionage with multiple purposes. To the extent that, according to Pierre Accoce, Romania managed to have a 13% rhythm of industrial development, the second one after Japan (Accoce, 1999, p.134). Given the context of the Cold War, the socialist system imposed and the Soviet pressure from above, Romania managed to walk as good as possible towards its aim of being a fully independent country. Through this network of spies and well-trained handlers, we have a fair image of the Romanian industrial espionage and its importance in achieving the often mentioned aims Romania focused on mostly during the second half of the Communist system.

Caraman network was fully dismantled in August 1969 after the defections of first, Evgheni Runge, a Soviet lieutenant-colonel that managed to pass to the West in October 1967, as his life was, allegedly, at threat, and furthermore of the general Ion Iacobescu, who was part of the network. Runge told the US Central Intelligence Agency (CIA) everything he knew about the network and the espionage activities of the East towards the West, generally. Nonetheless, the CIA just instructed the DST agents to keep a close eye on the Romanian Embassy in Paris. Without their defection, it is unlikely that the Caraman network would have been discovered in 1969. According to general Ion Iacobescu, Caraman received from Ceausescu the task of attracting and bringing back to the country all the scientists that left Romania. However, due to lack of information related to the outcome of this task it cannot be

confirmed if the network was successful in this matter. Such a task also proves the strategic importance of the industrial espionage in communist Romania.

Ultimately, Mihai Caraman returned to Romania and continued his service within the *Securitate* until 1979 when he was asked to retire. After the fall of the communist system in 1989, he was appointed adjunct to the Minister of National Defence and Commander in Chief of the Centre of External Intelligence (*Centrul de Informatii Externe – CIE*), nowadays known as the Foreign Intelligence Service (*Serviciul de Informatii Externe – SIE*). The actions of the Caraman network had longstanding consequences for the soon to be democratic country. In 1992, NATO warned Romania that having Mihai Caraman at the lead of the newly ´reformed´ *CIE* was going to diminish the Romanian efforts in advancing towards its membership of the Alliance.

The limited space for the presentation of this study does not allow us to give a more insightful perspective of the actions of the Caraman network, through relevant examples. These would show the methods and techniques used by Caraman to obtain the needed intelligence.

Conclusion

Cristian Troncota appreciated that the history of the twentieth century proved, especially for the small and medium states with more limited interests, that the full commitment of the secret services in pursuing the aims established by the government brought the country to the fulfilment of its aim. Regardless, the Romanian Revolution of 1989 raises questions on the actual fulfilment of the Romanian aim of 'independence' of the Soviet Union. By the end of his dictatorship, Nicolae Ceausescu has reportedly managed to pay Romania's entire external debt, which might be an indicator of the status of 'full independence' from the Soviet Union and other Western actors. However, his removal from power and the allegations of external involvement in the Romanian Revolution, that later appeared, raise an important question mark on the actual autonomy of the Romanians.

Even though the industrial espionage was a strategic objective of the communist system, the limited information obtained on it and the short analysis of it, proves the deficits of the Romanian communist system. Its importance in Romania might be attributed to Romania's link to the USSR. For the latter, the industrialisation was an important objective to achieve, to ultimately win the Cold War. For the Romanians, the industrial espionage was a tool of the technical and scientific revolution they were aiming at, according to primary sources.

A major reference of the paper is the study case on the Caraman network as the most successful achievement for this matter. The limited resources explaining this objective gave a confined perspective of its real importance for the Romanian government at the time. Its results distracted the USSR from the actions taken by the Romanians to ´clean´ the secret services of Soviet agents. Also, the industrial espionage, was used as a strategic weapon to develop the Romanian industries and scientific areas so the country could face easier the awaited rupture with the Soviets.

The thorough analysis of the research suggests that the communist system had the industrial espionage as a strategic objective between 1965 and 1989. The first objective of industrialisation established by the Romanians was fulfilled given the pace at which Romania had grown in this period, which in great part happened as a result of the intelligence gathered through industrial espionage. Many historians support the fact that providing the USSR with intelligence gathered from their espionage activities was part of the Romanians' strategy of distracting the Soviet overlord from their plan of independence. However, the historical findings suggest that the Romanians were conditioned by the Soviets to maintain their level of collaboration in the espionage activities in exchange of the withdrawal of the Soviet counsellors from their country. Such a mixture of hypothesis drives us towards the conclusion that the Romanians shrewdly managed to integrate their obligations towards the Soviet Union in their strategy. It has been mentioned previously that the importance of the industrial espionage was linked to the relation Romania had with the USSR. This was so for many reasons. First, would be the already explained strategy of distracting the Soviets from the internal restructuring. The industrialisation of the country, inspired by Soviet values in its initial stage, was also a tool of defence in order to be able to face the Soviets after the potential rupture. Also, the intelligence the Romanians obtained from their collaboration with the Soviets contributed significantly to the development of the industrialisation. So, in spite the often-mentioned desire to break free from Soviet influence, the Romanians used it as a weapon to achieve the eventual rupture.

As in the communist system the objectives were established during the process rather than before it, the industrial espionage became a strategic objective once the Romanians started to notice the facility they had in pursuing it.

The successful Romanian espionage activities between 1965 and 1989 were supported by some major happenings and circumstances. An example is the proposal of Yuri Andropov, in 1964, of a cooperation plan between the states of the Warsaw Pact. This plan suggested that the secret services of the

socialist countries would not focus on the total espionage but on limited issues and interest zones. In the meantime, the KGB would cover the general issues. This aspect is a potential explanation of the continuous restructuring of the *Securitate* and its focus on specific parts of the world rather than different issues, after 1965. Andropov's plan also mentioned the requirement of sending the full amount of intelligence gathered to Moscow rather than just synthesis of it. The denial of these proposals by the Romanian delegation after the retirement of the Soviet counsellors from Romania, increased the vigilance of the Soviets, but the Romanians expected it and were prepared to face it.

In the case of the Caraman network, as one of the most successful operations of industrial espionage from 1965-1989, there were several elements that facilitated espionage activities. First, the hate that General Charles de Gaulle nourished for the Americans helped the context in which a socialist country could have developed espionage activities. General de Gaulle was also looking for a hidden ally in the East.

Second, the fact that the intelligence gathered by the Caraman network and shared with the Soviets had a high quality facilitated an independent action with no involvement of the KGB. Therefore, the Romanians could manipulate easily the intelligence that reached Moscow as part of their obligation.

Third, the resources the Romanians, without Soviet contribution, invested in the operation were considerable and obvious, especially in the awards offered to their spies as well as in the facilities the diplomats had. Additionally, the fact that Romania had no reluctance in sharing the intelligence gathered by their own resources with the USSR, gives an interesting clue of the quality and importance of the intelligence shared with them in the first place. However, it is worth mentioning that the large investment in the actions of the secret services ended up affecting the population's wellbeing and furthermore it had a fatal effect on the system itself.

Fourth, the historical context of the Cold War and the fast-paced espionage activity that all the countries were engaged in, helped Romanian espionage activities to develop according to the country's needs. In this situation, is understandable why the Romanians had the industrial espionage as a strategic objective of the communist system. In their wish to outstand, to have a say, to be powerful when they had the resources, the means and the people to achieve that, it is not questionable why the Romanians pursued at such an intensity the espionage activities and particularly the industrial espionage between 1965 and 1989. Their potential to develop their industry was diminished by the Soviet interference and demands and that was only to be ended up with by growing stronger. The democratic countries had already

decades of development ahead. Thus, the Romanians had to focus their attention and skills towards them.

References:

1. Accoce, Pierre, (1999), *Rețeaua Caraman: cei treisprezece informatori care au zguduit NATO*, Compania.

2. Deletant, Dennis, (2001), *The Securitate Legacy in Romania*, in Williams, K. and Deletant, D., *Security Intelligence Services in New Democracies*, New York: Palgrave.

3. Deletant, Dennis, (1998), *Ceaușescu și Securitatea: constrângere și disidență in România anilor 1965-1989*, Bucharest: Humanitas.

4. Hossu Longin, Lucia, (2009), *Față în față cu generalul Ion Mihai Pacepa*, Bucharest: Humanitas.

5. Pacepa, Ion Mihai, (1999), *Cartea Neagră a Securității*, Volume 1, Bucharest: Omega.

6. Pacepa, Ion Mihai, (2013), *Moștenirea Kremlinului: rolul spionajului în sistemul communist de guvernare*, Bucharest: Humanitas.

7. Pacepa, Ion Mihai, (1988), *Red Horizons*, London: Heinemann.

8. Țăranu, Liviu, (2009), *Ion Mihai Pacepa în dosarele Securității, 1978-1980*, Bucharest: CNSAS.

9. Troncotă, Cristian, (2003), *Duplicitarii. Din istoria serviciilor de informații și securitate ale regimului comunist din România, 1965-1989*, Bucharest: Elion.

10. Troncotă, Cristian, (2006), *Torționarii, Istoria instituției Securității regimului comunist din România (1948-1965)*, Bucharest: Elion.

11. Banu, Florian, (2010), "Infiinţarea Departamentului de Informații Externe", in *Caietele CNSAS*, Anul III, nr. 1(5), Ed. Consiliul Național pentru Studierea Arhivelor Securității – CNSAS, Bucharest.

12. Banu, Florian, (2015), "Nicolae Doicaru – un cursus honorum enigmatic", *Caietele CNSAS*, Anul VII, nr. 1(13), *CNSAS*, Bucharest.

13. Bouillon, Pierre, (2014), "A Paradox in Computer Science: French and Romanian Cooperation during the Cold War", *International Committee for the History of Technology (ICOHTEC)*, Vol. 20, No. 2, pp. 115-124.

14. Ciobanu, Monica, (2011), "Rewriting and remembering Romanian communism: some controversial issues", in *Nationalities Papers*, 39:2, pp. 205-221.

15. Ciungu, Lavinia Corina and Kahn, David, (2015), "A Historical Survey of Romanian Intelligence, in *Cryptologia*, 39:2, pp.105-120.

16. Deletant, Dennis, (1995), "New Light on Gheorghiu-Dej's Struggle for Dominance in the Romanian Communist Party, 1944-49", in *The Slavonic and East European Review*, Vol. 73, No. 4, pp. 659-690.

17. Dennis Deletant, (1993), "The Securitate and the Police State in Romania: 1948–64", in *Intelligence and National Security*, 8:4, pp.1-25.

18. Dennis Deletant, (1994),"The Securitate and the Police State in Romania, 1964–89´, *Intelligence and National Security*, 9:1, pp. 22-49.

19. Granville, Johanna, (2010), "Blame the Messenger? Bucharest and Its Bungling Diplomats in 1956´, *Canadian Slavonic Papers*, Vol. 52, No. ¾, pp. 299-330.

20. Negoiță, Marian, (2011), "State Weakness in Post-Communist Romania and the Legacy of Communism", *Journal of Global Initiatives:Policy, Pedagogy, Perspective*: Vol. 6: No. 2, Article 6.

21. Stan Lavinia and Zaharia, Rodica Milena, (2007), "Romania's Intelligence Services: Bridge Between East and West?", in *Problems of Post-Communism*, 54:1, pp. 3-16.

22. Țăranu, Liviu, (2008), "Evoluția spionajului românesc după defecțiunea Generalului Ion Mihai Pacepa 1978 – 1989", *Anuarul Muzeului Marinei Române,* tom XI, pp.282-294.

23. "Caracterul științific al activității de securitate desfășurate pentru cunoașterea, prevenirea și contracararea oricăror acțiuni ostile a faptelor și fenomenelor care pot genera sau favoriza comiterea de infracțiuni împotriva Securității Statului", *Departamentul Securității Statului*, Ministerul de Interne, Consiliul Național pentru Studierea Arhivelor Securității – CNSAS, http://www.cnsas.ro/documente/materiale_didactice/D%20008712_001_p40.pdf.

24. "Din tainele serviciilor secrete", (1976), *Serviciul cultural, presa și editorial,* Ministerul de Interne, CNSAS, http://www.cnsas.ro/documente/materiale_didactice/D%20001528.pdf.

25. Decretul nr. 295 din 3 aprilie 1968, *Monitorul Juridic, (Bucuresti, 1968),* http://www.monitoruljuridic.ro/act/decret-nr-295-din-3-aprilie-1968-privind-infiintarea-organizarea-si-functionarea-consiliului-securitatii-statului-emitent-consiliul-de-stat-publicat-46499.html.

26. "Ofensiva spionajului economic", (1973), *Oficiul pentru propagandă, publicații de specialitate și editorial*, Ministerul de Interne, CNSAS, http://www.cnsas.ro/documente/materiale_didactice/D%20001451.pdf.

27. "Războiul din umbra", (1969), *Direcția învățământ*, Consiliul Securității Statului, Consiliul Național pentru Studierea Arhivelor Securității – CNSAS, http://www.cnsas.ro/documente/materiale_didactice/D%20017448_014.pdf.

28. "Războiul nevăzut", (1970), *Direcția personal și învățamânt*, Consiliul Securității Statului, Consiliul Național pentru Studierea Arhivelor Securității – CNSAS, http://www.cnsas.ro/documente/materiale_didactice/D%20001453.pdf.

29. "Rețele informative", (1969), *Direcția învățământ*, Consiliul Securității Statului, Consiliul Național pentru Studierea Arhivelor Securității – CNSAS, http://www.cnsas.ro/documente/materiale_didactice/D%20001464.pdf.

EASTERN AND CENTRAL EUROPE IN THE COLD WAR PERIOD: THE SOVIET MODEL OF INTELLIGENCE STRUCTURES

Bogdan Alexandru TEODOR*
Mihaela TEODOR*

Abstract

An ideological clash between Soviet communism and American anti-communism was central to the Cold War conflict. American policymakers, such as George Kennan and John Forest Dulles, acknowledged that the Cold War was essentially a war of ideas; a war largely fought out on two fronts: intelligence and propaganda.

Since the late 1940s, in Eastern and Central Europe, institutionalized intelligence organizations resulted from direct subordination to a foreign state secret service, the Soviet one. After the World War II the Red Army and NKVD units were present at the organizing session of all intelligence services in Eastern and Central Europe (Bulgarian, Czechoslovak, East German, Hungarian, Polish, and Romanian). It was copied the Soviet security apparatus model, their structure and operational guidelines were based on verbatim translations from Russian documents. This paper aims to provide a short overview of intelligence structures evolutions in Eastern Europe during the Cold War, in order to highlight some important moments in the history of "institutional (in) dependence" on the Soviet Union for most of these structures.

Keywords: *Cold War, Intelligence, soviet model, Eastern and Central Europe*.

Introduction

In Eastern and Central Europe institutionalized intelligence structures resulted from direct subordination to a foreign state. Since late 1940's, Bulgarian, East German, Czechoslovak, Hungarian, Polish, and Romanian intelligence structures had been subordinated to the Soviet intelligence service. This paper aims to provide a short overview on evolutions of intelligence organizations in Eastern Europe during the Cold War, in order to

* Associate Professor Dr. "Mihai Viteazul" National Intelligence Academy.
* Senior Researcher Dr. National Institute for Intelligence Studies.

highlight some important moments in the history of "institutional (in) dependence on the Soviet Union" for these intelligence structures.

The Soviet Model of Intelligence

As Alexander Orlov stressed in 2007, in his paper "The Theory and Practice of Soviet Intelligence", Soviet intelligence structure based its work "100% on secret sources and undercover agents". Thus, the army intelligence main efforts were concentrated "on building and operating networks of secret informants" (Orlov, 2007).[1] In this respect, the same author highlights the *essence of the Soviet doctrine of intelligence*: "Important state secrets and especially clues to the intentions and plans of potential enemies cannot be found in libraries or encyclopaedias, but only where they are kept under lock and key. The task of intelligence services is to acquire the keys and deliver the secrets to their governments, thus providing them with the foreknowledge and orientation needed for the making of decisions." (Orlov, 2007)

To understand the specific of the Soviet intelligence, in the following table, we propose a short evolution timeline of the Soviet intelligence structures.

Table 1: Soviet Secret Service Evolution Timeline (1917-1953)[2]

Period	*Abbreviation*	*Organization Name (English)*	*Important moments*
1917	*NKVD*	*People's Commissariat for Internal Affairs*	*1917 – New Bolshevik government formed NKVD*
1917 - 1922	*Cheka*	*"All Russian Extraordinary Commission for Combating Counter-Revolution and Sabotage"*	*December 1917 – was established - The first Soviet Union security organization called Cheka later known as Vacheka*
1922 - 1923	*GPU*	*State Political Directorate*	*1922 abolition of the Vcheka, formed GPU*

[1] "The Main Intelligence Department of the Army did study some legitimately accessible sources, but only those dealing with military matters, such as foreign military and scientific journals, army and navy manuals, military textbooks, topographic explorations, and anything printed anywhere about the armed forces of the world". See more at Orlov, 2007.

[2]Source: CIA Interim Report, June 1948, https://www.cia.gov/library/readingroom/document/cia-rdp78-02546r000100130001-3.

1923 - 1934	*OGPU*	*Unified State Political Directorate*	*1930 NKVD officially abolished*
1934 – 1943	*NKVD*	*People's Commissariat for Internal Affairs*	*1934 – NKVD reinstated as an all-union agency of executive power* *1941 – NKGB was subordinated into NKVD*
1943 – 1946	*NKGB*	*People's Commissariat for State Security*	*1941 - decree 149 of the CPSU Politburo creating NKGB* *1943 – a decree issued splitting the regular and political police into two agencies and resulted in a creation of the NKGB, which gradually transferred all security and law enforcement functions from the NKVD.* *March 1946 – NKGB renamed – MGB and NKVD renamed MVD*
1946 – 1954	*MGB*	*Ministry of State Security*	*March 15, 1946 – NKGB became MGB*
1946 – 1954	*MVD*	*Ministry of Internal Affairs*	*March 13, 1954 – the Ministry for State Security was transformed in the Committee for State Security or KGB (MVD and MGB amalgamated into one organization)*
1954 – 1991	*KGB*	*Committee for State Security*	*1991 Soviet-era ministry, merging three security bodies into one FSB with the Foreign Intelligence Service (SVR) and the majority of units of the Federal Protection Service (FSO), which oversees the protection of the country's top leaders*

In 1941, was created the People's Commissariat for State Security (NKGB), responsible for external espionage, counter-espionage, and guarding the leaders of the party and state. However, in 1946, for political and propaganda reasons, all Peoples' Commissariats were renamed ministries and NKGB became Ministry of State Security (MGB). Thus, internal security and foreign intelligence were joined in a single ministry, which integrated all the

intelligence functions formerly performed by both ministry and all the security functions of Ministry of Interior (MVD). MGB was the model for all intelligence organizations from satellite states (CIA Interim Report, June 1948).

First created in 1946, the MGB was responsible for internal and external intelligence activities, being a rival to the Interior Ministry, having taken away some of the functions of the latter. The MGB was liquidated on March 13, 1954, being transformed in the Committee for State Security or KGB (CIA Interim Report, June 1948).

Formal control: In theory, the MGB was responsible to the Council of Ministers, formerly the Council of Peoples' Commissars of the Soviet Union. In fact, the MGB was responsible only to Stalin and the Politburo.

Organization: The CIA repost prove that, the main departments of Soviet intelligence structure included various departments: political, military, and economic intelligence; evaluation and requirements; and administration. MGB was organized in several main directorates: Directorate of Intelligence; Directorate of Counter-Intelligence; Secret Political Directorate and Directorate of the Commandant of the Moscow Kremlin. In many fields the MGB operates jointly and almost as a single agency with the Ministry of Internal Affairs (MVD) (CIA Interim Report, June 1948).

Functions: MGB was responsible for intelligence, counterintelligence and the protection of the government, being engaged in more lines of intelligence activity and related work.

The first line, the "diplomatic intelligence", which was considered the most important, was done in order "to keep the Soviet government informed of the secret deals between the governments of capitalistic countries and of the true intentions toward the Soviet Union" (Orlov, 2007).

The second line was: "to procure data on the military posture of Western and other countries, the quality and strength of their armies, navies, and air forces, their degree of mechanization, mobility, fire power, technological advancement, and modernization, and the productive capacity of the armament industries and the mobilization plans of the big powers" (Orlov, 2007).

The third line was called economic intelligence, which "was created for the purposes of exercising State control over Soviet export and import operations and of protecting Soviet foreign trade from the pressures and abuses of international cartels and other organizations of monopolistic capital" (Orlov, 2007).

The fourth line was: "misinforming and misleading the foreign governments concerning its own position and intentions" (Orlov, 2007).

The fifth line was the activity of infiltration into the foreign security agencies and intelligence services.

As Olov (2007) affirm: "The penetration of foreign *intelligence* services was done to find out whether they have succeeded in creating a spy network in Soviet Russia, and if so who these spies are, what secret information they have transmitted, and what lines of communication they use."

The sixth line was: "to influence the decisions of foreign governments through secret agents occupying important positions within them" (Orlov, 2007).

The Soviet sphere of influence and the Soviet intelligence

After the World War II, The Red Army (SMERSH)[3] and MGB units were present at the organizing session of all intelligence services in Eastern and Central Europe; during wartime, military intelligence becoming the principal activity of every branch of the Soviet Intelligence structures.

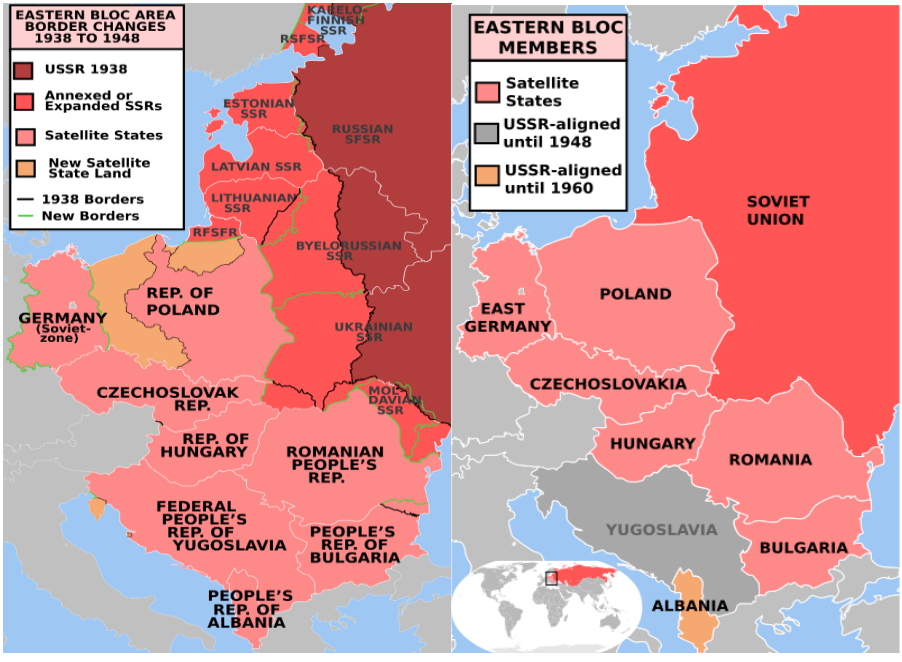


Figure 1: Map of Soviet sphere of influence in Eastern and Central Europe with border changes resulting from military operations of World War II and the Eastern Bloc[4]

[3] Special units of the People's Directorate of Interior of USSR were called SMERSH.
[4] Source: https://en.wikipedia.org/wiki/Military_occupations_by_the_Soviet_Union.

As Alexander Orlov (2007) stressed: "While the *residenturas* abroad kept the government informed of the enemy's grand strategy and his capabilities and vulnerabilities, day-to-day tactical or combat intelligence was taken care of by the intelligence sections of the Soviet armed forces and by the special detachments of the MGB attached to all army units down to the regimental level." Thus, the Soviet intelligence officers were omnipresent as "advisers" making sure that the fraternal services carried out Moscow's orders. Moreover, it was copied the Soviet security apparatus model, their structure and operational guidelines "were based on verbatim translations from Russian documents". As we can see in the following table, the state department/directorate/ministry – was the name took by the intelligence structures in Eastern and Central Europe, as the soviet model MGB.

Table 2: Historical intelligence organizations
in Eastern and Central Europe during the Cold War[5]

Country	***Abbreviation State Security Agencies***	***Organisation Name English)***	***Organisation Name (Original)***
Hungary	*AVH*	*State Protection Authority*	*Államvédelmi Hatóság (formally merged into the Ministry of the Interior in 1953, abolished in 1956)*
Bulgaria	*DS*	*(Committee for) State Security*	*(Komitet za) dăržavna sigurnost*
Soviet Union	*KGB*	*Committee for State Security*	*Komitet gosudarstvennoĭ bezopasnosti*
Poland (to 1954)	*MBP*	*Ministry of Public Security*	*Ministerstwo Bezpieczeństwa Publicznego*
Poland (from 1954)	*SB*	*Security Service*	*Służba Bezpieczeństwa*
Romania	*Securitate*	*Department of State Security*	*Departamentul Securității Statului*
Albania	*Sigurimi*	*Directorate of State Security*	*Drejtoria e Sigurimit të Shtetit*

[5] Source: http://www.coldwareasterneurope.com/Overview/Communist-States-Fact-File/Organisations.

East Germany	*Stasi*	*Ministry for State Security*	*Ministerium für Staatssicherheit*
Czechoslovakia	*StB*	*State Security*	*Státní bezpečnost (Czech), Štátna bezpečnosť (Slovak)*
Poland (to 1954)	*UB*	*Office of Security*	*Urząd Bezpieczeństwa*
Yugoslavia	*UDBA*	*State Security Administration*	*Služba državne sigurnosti, Služba državne bezbednosti*

The East German case: Researchers agree that "the Soviets had a strong hand in the creation of the East German state security apparatus". The East German intelligence activities were conducted by the Ministry of State Security (MfS) of the German Democratic Republic (GDR), in East Berlin. The Ministry was founded in February 1950, the main purpose being "to contribute to consolidating the new Communist regime imposed on the population in the Soviet controlled zone of Germany" (Vermaat, 1987, p. 46). The functions, duties, main directorates, departments and smaller departments or units of the MfS derived from its detailed structure and operational focus. Initially, the Ministry of State Security had only domestic functions, espionage operations abroad being conducted by the "Institute of Economic Research" formally residing under the Ministry of Foreign Affairs. In the same time, the military intelligence operations were conducted by the Ministry of National Defence (MfNV). In 1956, for example, foreign intelligence operations were delegated to the "Chief Department of Intelligence" (HV A) within MfS (Vermaat, 1987, p. 47), which was considered the most successful spymaster of the Cold War. As Fischer stressed "the Soviet and East German secret services concentrate heavily on West Germany which was considered one of the most important targets in Europe; both Soviets and East Germans managing to penetrate the West German government apparatus, political parties and counter-intelligence service with great effect" (Fischer, 2014).

Institutional (in)dependence on the Soviet Union

During the Cold War period, the Soviet intelligence and its Warsaw Pact allies referred to each other as "brotherly or fraternal services"[6]. The

[6] Formally known as the "Treaty of Friendship, Co-operation and Mutual Assistance", the Warsaw Pact was created on 14 May 1955, after the accession of West Germany to the Nord Atlantic Alliance.

fraternal services in their organization and bureaucratic culture were more Russian than national, efficiency and contribution to Soviet intelligence being more important than national interest. For example Vermaat (1987) affirm that "a Soviet-East German protocol from 1978 revealed that Soviet officers were issued passes that allowed them unrestricted access to MfS and HV A offices, files, and technical equipment". Additionally to political and military intelligence, East European intelligence structures were tasked with collecting information on "nuclear weapons, nuclear energy, chemistry, electrical engineering, electronics, aviation, and conventional weapons" (Vermaat, 1987). These intelligence requirements were of overriding concern to Moscow. In this respect, only in the 1960's the Kremlin started to allow its trustworthy satellites, as East Germany and Romania, to "get involved in international affairs", under Soviet close supervision.

Moreover, as experts highlight, the Soviets and their Warsaw Pact allies have a long tradition of acquiring western technology by covert means. According to Orlov (2007), "Soviet technological advancements have only been made possible through meticulous and consistent intelligence gathering by the KGB and its sister services". However, beginning with the 1960s, "acquisition of scientific and technical intelligence in the West became a paramount objective both for the fraternal services and even more so for the KGB" (Fischer, 2014). Engineers, scientists, and inventors working in the foreign laboratories of the big industrial concerns of the world was recruited by Soviet intelligence (Orlov, 2007). For example, the "HV A managed to penetrate a number of firms and research centres like Siemens, Blohm, IBM, Hoechst and the nuclear research Centre in Karlsruhe" (Vermaat, 1987, p. 57). Although, the Soviet dependence on Western research and know-how was still extensive. Therefore, Western technologies were still a major target for Soviet and Eastern bloc intelligence.

The East German secret service is heavily involved in this effort: "as early as in 1970, the HV A created an entire "Sector for Science and Technology" (SWT) comprising three "operational departments" dealing with nuclear technology, microelectronics and the construction of engines and vehicles" (Vermaat, 1987, p. 57).

In the Cold War, according to intelligence experts, "the majority of industrial and technological espionage serves military purposes". Military intelligence also involves penetration of Western military establishments as NATO, Defence Ministry, US military headquarters in Germany, etc. (Vermaat, 1987, p. 58). According to Christopher Andrew and Oleg Gordijewski (1992), Soviet residents until 1976 were informed that European Community was not object of Moscow's interest. However, in late 70s the Central Committee of

CPSU recognized European Economic Commission as one of the „main object of intelligence penetration", putting it on the same level as USA, NATO and China. Moreover, "each allied service had to obtain KGB permission before developing an anti-US operation, and then the operation had to be cleared in advance by the KGB and serve KGB interests" (Orlov, 2007).

The Romanian case: "The General Directorate for the Security of the People" (DGSP) was officially founded on August 30, 1948, by "Decree 221/30 of the Presidium of the Great National Assembly" (Hitchins, 2014, p. 232). It was created with the help of Soviet SMERSH, the soviet counter-intelligence unit from Red Army, but it was copied the Soviet security apparatus model, their structure and operational guidelines were based on *verbatim* translations from Russian documents (Ministry of Internal Affairs Decision for the Organization of Department of State Security, September 2, 1948).

Table 3: Internal organization of Soviet and Romanian central intelligence apparatus[7]

THE SOVIET MODEL- MGB	ROMANIAN DEPARTMENT OF STATE SECURITY
•First Main Directorate - Foreign intelligence •Second Main Directorate - domestic counterintelligence and acted as an internal security and political police force •Third Main Directorate - military counterintelligence •Fourth Directorate – combat the anti-Soviet underground •Fifth Main Directorate - Main Secret Political Administration •Sixth Directorate - collect and process Signals Intelligence, or SIGINT •Seventh Directorate – Tehnic division •Division for the Protection of Leaders •Economic Administration	•First Directorate – intelligence •Second Directorate - counterintelligence or counter sabotage service •Third Special Directorate •Fourth Directorate - operative investigation •Fifth Directorate – secret political investigation •Sixth Directorate – the protection of leaders •Seventh Directorate - Tehnic division •Eight Directorate – Human resources •Ninth Directorate - The political education directorate •Economic Administration

[7] Source: https://en.wikipedia.org/wiki/Ministry_of_State_Security_Soviet_Union and http://www.cnsas.ro/documente/acte_normative/7346_003%20fila%20271-282.pdf.

As Rodica Gheorghe stressed in his thesis, "for the Cold War period, most scholars have discussed Romania's intelligence strength in term of its ability to suppress domestic dissent and to silence the Diaspora, with the final goal of insuring the survival of the communist regime." (Gheorghe, 2010, p. 14) However, according to the same author, "Romanian intelligence policy in the Cold War period also had an external dimension which raised concern in foreign intelligence agencies", including in the Soviet one.

Romania's "active diplomacy provided an official cover for his intelligence services to penetrate the Western and the Third World" (Gheorghe, 2010, p.6). Even if, in the first years of the Cold War the "Soviet intelligence established a strong foothold in Romania, – for instance the relationship between the Romanian Foreign Intelligence Directorate and the KGB was in the beginning stronger than between DIE and the Romanian government – Romania had made significant strides toward getting out from under Moscow's thumb in the 1960s" (Gheorghe, 2010). As Larry Watts (2007) straight in his paper, "this break ended the participation of Romanian intelligence officers in joint operations with the KGB". Moreover, repeated purges eliminated the Soviet counterintelligence capabilities within the Romanian Service. Bucharest even "went so far as to create departments that specialized in anti-KGB counterespionage, underscoring the difficult relationship with Moscow" (Larry Watts, 2007).

Conclusion

The Eastern and Central European intelligence structures ware creations of Soviet intelligence. In all Soviet Bloc countries, Soviet advisors and specialists deployed at individual ministries were the key instrument of Sovietisation of the Communist regimes. Their influence was frequently stronger than the word of ministers and other functionaries. The first advisors sent by the Ministry of State Security of the USSR (MGB) to Soviet Bloc countries came to oversee show trials and introduced various forms of repression into the security apparatus's methods. Thanks to a growing number of advisors and specialists, the intelligence structures became fully subordinate to MGB HQ in Moscow. In that way they helped create an international security apparatus run from Moscow that was able to operate independently throughout the Soviet Bloc. As Larry Watts stated in his article, the end of the Cold War raised problems for intelligence reform, after 89, the transition tent to favour the "destruction of intelligence apparatuses" (Watts, 2007), not their reform. The former Eastern Bloc intelligence structures have dissolved along with their Communist ruled states.

References:

1. Andrew, Christopher, Gordievsky, Oleg, (1992), "*More Instructions from the Centre: Top Secret Files on KGB Global Operations 1975–1985",* London.

2. Decree no. 221 from 28.08.1948 for the organization of General Directorate of People Security, The National Council for the Study of the Securitate Archives, collection M.I./D.M.R.U., file no. 7346, vol. 1, f. 7-8, accessible on-line on http://www.cnsas.ro/documente/acte_normative/7346_001%20fila%20007-008.pdf.

3. Fischer, Benjamin B., (2014), *Bruderorgane: the Soviet origins of East German Intelligence*, in "Ghi Bulletin Supplement", no. 9, pp. 151-169, accessible on-line on https://www.ghi-dc.org/fileadmin/user_upload/GHI_Washington/Publications/Supplements/Supplement_9/bu-supp9_151.pdf.

4. Gheorghe, Rodica Eliza, (2010), "*The Romanian Intelligence Services during the Cold War: how small powers can sometimes be strong"*, thesis submitted to the Faculty of the Graduate School of Arts and Sciences of Georgetown University in partial fulfilment of the requirements for the degree of Master of Arts in Security Studies, Washington, DC, April 16, available on-line on, https://repository.library.georgetown.edu/bitstream/handle/10822/553496/gheorgheRodica.pdf.

5. Grunova, Alexandra, (2008), "NKVD/KGB activities and its cooperation with other Secret Services in Central and Eastern Europe 1945-1989". Anthology of the international conference Bratislava 14-16 November 2007, Nation's Memory Institute, Bratislava.

6. Hitchins, Keith, (2014), *A Concise History of Romania*, Cambridge University Press.

7. Ministry of Internal Affairs Decision for the Organization of Department of State Security, September 2, 1948, the National Council for the Study of the Securitate Archives, collection M.I./D.M.R.U., file no.7346, vol. 3, f. 271-282, accessible on-line on accessible on-line on http://www.cnsas.ro/documente/acte_normative/ 7346_003%20fila%20271-282.pdf.

8. Orlov, Alexander, (2007), The Theory and Practice of Soviet Intelligence, accessible on-line on https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol7no2/html/v07i2a05p_0001.htm.

9. Semukhina, Olga B., Reynolds, Kenneth Michael, (2013), *Understanding the Modern Russian Police*, CRC Press, pp. 57-67, accessible on-line on https://www.systemaspetsnaz.com/history-of-the-cheka-ogpu-nkvd-mgb-kgb-fsb.

10. *"Soviet Intelligence, Organization and Functions of the Ministry of State Security (MGB)"* Interim Report, June 1948, General CIA Records, available on-line from November 2016 on https://www.cia.gov/library/readingroom/document/cia-rdp78-02546r000100130001-3.

11. Vermaat, J.A. Emerson, (1987), "*The East German Secret Service Structure and Operational Focus"*, in "Conflict Quarterly", Fall, pp. 46-62.

12. Watts, Larry, (2007), "*Intelligence Reform in Europe's Emerging Democracies"*, Conflicting Paradigms, Dissimilar Contexts, Posted: April 14, 2007 on https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/ studies/vol48no1/article02.html.

INTELLIGENCE AND SECURITY IN THE 21ST CENTURY

A RAWLSIAN APPROACH TO DE-SECURITIZATION

Valentin STOIAN-IORDACHE*

Abstract

Practices of contesting security have been identified by several authors, such as Claudia Aradau, Florent Blanc or Matt Mcdonald in actions ranging from protests against the Iraq war, Roma people cleaning up trash, the re-shaping public discourse on security and judicial contestation of national security policies. The paper first criticizes the practices of contesting security that the literature has uncovered by focusing on their insufficiently deliberative character. It argues that securitization theory, as originally formulated by the Copenhagen school, opposed the logic of security to the logic of deliberation. Thus, the paper concludes that these practices include a type of non-public reasons which a real deliberative democracy would exclude.

Alternatively, the paper looks to the concept of public reason as formulated by political theorist John Rawls as a better understanding of how de-securitization should proceed. It argues that only public reason-giving practices, such as judicial contestation can amount to a true de-securitization.

Keywords: *securitization, Rawls, Copenhagen school.*

Introduction

The meaning of the term security, as well as its normative legitimacy and strategies to achieve or escape it has been the subject of a significant level of contestation in recent literature. From an analytical point of view, the very understanding of the term "security" is highly debated, as well as the explanation of the emergence of security phenomena. From a normative point of view, the controversy is more muted, but the crux of the matter under debate is whether using the standard means of security policy helps or harms marginalized groups such as immigrants, sex workers or nomadic communities.

* Researcher dr. within National Institute for Intelligence Studies, valentin.stoian@animv.ro..

The discourse of security institutions understands the idea of "security" as a "state", in which threat is absent. The probability that threats might be actualized has to be evaluated and then the most significant potential threats need to be removed. At the same time, critical academic work identifies resistance to security with a set of practices by marginal groups, who are either directly; threatened by security policies or who, for reasons of institutional ideology, critically engage with the security apparatus. Yet, similarly to the discourse generated by security institutions, practices of resistance suffer from a flaw which this article aims to expose and criticize.

The article will offer a Rawlsian account of de-securitization, grounded in the idea of public reason and deliberative democracy. It argues that emancipation and resistance practices as described by the literature suffer from the same weakness that the discourse of security institutions: an insufficiently deliberative character caused by the use of private rather than public reasons. Alternatively, if emancipation is supposed to fulfil the promise its original proponents made, then it must not exhibit the same weaknesses as that which it opposes.

The account of emancipation which the article supports relies on John Rawls' idea of public reason. John Rawls (1996: 224) describes public reason as both a characteristic of the relationship of the state to the individual and as a set of guidelines of inquiry which apply to citizens generally, but particularly strong to public officials, candidates for public office and above all, constitutional judges. The key element of the latter conception is the prohibition of using non-public reasons (reasons which are grounded in particular comprehensive doctrines which begin from premises which not all members of society could accept) when arguing for a public policy which will coercively be imposed on all.

The first section carries out a review of the literature on moral reasons for de-securitization and of practices associated with opposing and contesting security. It argues that while there are compelling moral reasons for de-securitizing (exiting the logic of security), practices associated with doing so have many times carried on the same non-deliberative approach that security discourse is engaged in. Rather than contest security by dialogically undermining its discursive bases, practices of resistance and emancipation have followed the same use of non-public reasons as practices and discourses of security.

The second section outlines the idea of public reason as described by John Rawls in *Political Liberalism* and the *Idea of Public Reason Revisited.* According to Rawls, the duty to use only public reason is incumbent on officers of government, while the exemplar of public reason in a society is its

judicial body entrusted with interpreting the constitution. The prohibition of non-public reasons as grounds for argumentation is especially emphasized in this section, as well as the idea of the Supreme Court as an exemplar of public reason. The section places security, understood as the Schmittian politics of exception in direct opposition of the notion of public reason.

The third section outlines, through an analysis of policy document, laws and public statements, as well as two pieces of grey literature, the process of securitization of corruption in Romania. The fourth constitutes a case study of two Romanian Constitutional court decisions which removed critical parts of security legislation. The first eliminated intelligence services from participating in criminal investigations while the second struck down a highly ambiguous article on the law of national security. The Constitutional Court is analysed as a public-reason based de-securitizing actor and its arguments for striking down the laws as an example of judicial public reason.

Is securitization desirable and if yes, how?

The literature on securitization and de-securitization has gradually moved towards the overwhelming position that securitization theory has a clear normative approach and that de-securitization is normatively desirable. Roe (2012) summarizes the literature on securitization and de-securitization and identifies three main approaches to the normative justification of de-securitization: the process approach, the outcome approach and the indeterminate/utilitarian approach. According to the first, securitization in undesirable because issues should be dealt with, as much as possible, through the means of normal politics, as opposed to silence and speed, which leads to decisions being taken by a privileged elite of security professionals (Roe 2012: 252). On this view, normal politics is understood as deliberative and open, subjecting controversial issues to debate and allowing time to have all voices heard.

This approach seems to have textual support in the Copenhagen school's main text: *Security a new framework for analysis,* as well as in other works published by Ole Waever. The authors of *Security a new framework for analysis* present two definitions of politicization, leaving ample place for ambiguity on their understanding of its opposite. On the one hand, they define the existence of a continuum from non-politicized to securitized, claiming that: *any public issue can be located on the spectrum ranging from non-politicized […] through politicized (meaning the issue is part of public policy, requiring government decision and resource allocations or, more rarely, some other form of communal governance) to securitized (meaning the issue is presented as an*

existential threat, requiring emergency measures and justifying actions outside the normal bounds of political procedure) (Waever et all. 1998: 23).

While, only six pages later, they understand the politicized situation as: *"Politicization means to make an issue appear to be open, a matter of choice/something that is decided upon and that therefore entails responsibility, in contrast to issues that either could not be different (laws of nature) or should not be put under political control (e.g.* a free economy* the private sphere, and matters of expert decision)* (Waever et all. 1998: 29).

Waever seems to offer support for the deliberative understanding of politics in his 2011 article, where he argues that "the theory has a Schmittian concept of security and an Arendtian concept of politics" (Waever, 2011, 470). According to Waever: "*Hannah Arendt (1958, 1968, 2005) insisted that politics is productive, irreducible and happens among people as an unpredictable chain of actions….Therefore, the definition of securitization shapes every usage of the theory and entails this Arendtian concept of politics, because the theory places power in-between humans – not least through the central role of the audience – and insists on securityness being a quality not of threats but of their handling, that is, the theory places power not with 'things' external to a community but internal to it"* (Waever, 2011, 468).

The second approach to justifying de-securitization quoted by Roe (2012) is that favoured by Claudia Aradau (2003, 2008), Jeff Huysmans (1998a, 1998b, 2006) and Didier Bigo (2002). Similarly to Waever, these authors link security politics to the work of Carl Schmitt (or, alternatively to that of Giorgio Agamben) and his description of the political in terms of friend and enemy. They fault securitization for creating exclusionary logics, eliminating migrants and other undesirables from the proper scope of the political community. Given her understanding of security as "barred universality", Aradau (2004, 2008) criticizes securitization, but also the Welsh school view of emancipation, for perpetuating an exclusionary logic. Similarly, Huysmans (1998a, 1998b, 2006) argues in favour of de-securitization on philosophical grounds. He understands "security" in wide sense, as a technique of government meant to define the "us" versus the "them", through the production of subjects whose minds are infused with Hobbesian images of death being permanently near. He relies on the Schmittian nature of security, which is populated by distinctions between friend and enemies to argue in favour or de-securitization as the normatively preferred strategy. Huysmans quotes the history of racism and exclusionary policies in the West as arguments to reject any form of othering and to favour universality as the normatively desirable strategy. Finally, Bigo (…) looks as the formation of the practices and discourses of the "managers of unease" (the security

professionals entrusted with handling the issues of security) and criticizes the instantaneity intrinsic in the model of securitization that the original Copenhagen school proposes. According to Bigo (…), the fact that security practices and discourses are entrusted to security professionals who are socialized in exclusionary logics, poses a significant threat to the universalist promise of contemporary liberal democracies.

Finally, the utilitarian approach argues that securitization or de-securitization are desirable according to the effects they produce. Thus, in the view of Rita Floyd, some problems such as environmental issues are better dealt within a security framework, while for others, the logic of normal politics is best appropriate. Floyd (2007a, 2007b, 2010, 2015) offers a utilitarian-inspired theory of securitization, where a specific act of securitization is normatively justified if it meets five conditions: the existence of an objective existential threat, right of referent objects to defend themselves or to defensive assistance (where human being are by definition entitled to protection, while the other sectors have to be proven to help with the realization of human needs, right intention for securitization, overall higher good from securitization, more security as opposed to insecurity being produced from the particular securitization) (Floyd 2015: 123).

While there seems to be a consistent agreement in the literature that de-securitization is normatively desirable, the varieties of contesting security seem endless. Most authors discuss the appropriate strategies to de-securitization, while fewer focus on what lies at the opposite end from security. Both groups believe that contesting security is helpful and even necessary, but disagree on how exactly this is to be done. This article evaluates some of these proposed de-securitizations but finds them wanting given their insufficiently deliberative character, thus making them closer to practices of security.

Claudia Aradau (2004, 2008, 2015) criticizes both the practice of securitizing the plight of the excluded (such as trafficked women) and the Welsh school's idea of equating emancipation with security. Alternatively she sees emancipation in practices such as anti-war protests under the banner "not in my name" (2004), meetings of sexual workers which adopted a declaration of rights (2008) and communal rubbish collection in a Roma camp in France (2015). While protesting the declaration of war in Iraq under the "not in my name banner" or demanding the rights of sex workers could be seen as deliberative forms of contestation, they fail to engage and criticize the securitizing discourse they aim to challenge. Aradau (2008:191) argues correctly that "Politics out of security starts from a shedding away of particularity, from a suspension of classification and representation", yet the

practices that she outlines as doing so fail in their assumed goal. Aradau's exemplars of de-securitization only look to affirm and challenge the framing of a discourse, but are unsuccessful in engaging the premises and logics of inference that securitizing speech undertakes. Rational debate on shared premises is impossible if contestation is nothing but a battle of discourses struggling to offer different frames to the same reality.

A similar weakness is exhibited by the practices outlined by a long series of other studies. Matt McDonald (2015) looks at how pro-refugee NGOs in Australia contested security through reshaping the discourse on it and framing the desirable policy goals as the "human security" of migrants rather than the security of Australians from migrants. Piazza (2015) describes how student groups resisted the introduction of biometric cards by framing the discourse on them as discourses of control, racist-based anthropometry, corruption of childlike innocence and Nazism. Similarly, Rygiel (2011) outlines the way in which pro-migrant NGOs contest the discursive exclusion of migrants from the Calais "jungle". She argues that a form of universal citizenship-based articulation of grievances achieves the integration of excluded migrants in form of community and contests their Agamben-ian banishing from the political community. A similar articulation of contestation in the Calais "jungle" is found in Rigby and Schlembach (2013) who focus on migrant protest and universalism-based formulation of claims.

Finally, de-securitizations that involve a "high politics" approach are described by Balzacq, Depauw and Leonard(2015) and Blanc (2015). The first look at how an EU directive was changed to allow intra-EU arms trade, thus taking away licensing rights from national governments, while the second analyse legal challenges to the US Patriot Act and indefinite detention in the Guantanamo Bay prison camp. However, none of these studies focus on the express arguments which were invoked in favour of the de-securitizing approach, with the limited exception of the ideas invoked by lawyers of Guantanamo bay detainees that international law should also apply in war (Blanc 2015: 78).

The idea of public reason

In his two classic works, *Political Liberalism* and *The Idea of Public Reason Revisited,* John Rawls grapples with the Rousseau-ian problem of how can citizens, who are equally free, at the same time be bound by coercively imposed laws. To complicate matters, he also introduces the notion of reasonable pluralism (the fact that citizens share different comprehensive doctrines). His answer is a version of political liberalism, understood as a

political as opposed to a moral conception of justice, which is supported by an overlapping consensus - the fact that the society's common political conception is supported by reasons internal to each comprehensive doctrine. Public reason is, then, the way that democratic citizens need to relate to each other politically in such a society.

Overall, the idea of public reason could be defined as the way in which citizens in a liberal society and especially officers of government have to argue for decisions that are to be coercively imposed. Rawls demands that they must argue from reasons and use rules of inference that everybody can accept. Therefore, he excludes aspects such as the private reasons of churches and associations from public debates. These, while they can be invoked to bolster an argument, cannot form the ground for a justification of coercively imposed measures.

John Rawls does not offer a concrete and explicit definition of the term "public reason" in any of his works on the topic**.** Alternatively, he discusses the idea of public reason as a way in which a society "puts its ends in an order of priority and makes its decisions accordingly" (Rawls 2005[1993], 212), or "a relationship of persons within the basic structure of the society in which they are born and in which they normally lead a complete life" (Rawls 2005[1993], 216). Further, while eschewing what public reason actually is, Rawls defines it according to what it does, as it "specifies at the deepest level the basic moral and political values that are to determine a constitutional democratic government's relation to its citizens and their relation to one another. In short, it concerns how the political relation is to be understood" (Rawls 1999, 132). Finally, Samuel Freeman describes public reason as it involves a set of shared considerations which count as good reasons in public deliberation and argument about laws and their interpretation, among reasonable and rational democratic citizens who endorse different fundamental values" (Freeman 2004, 2027).

Rawls then proceeds to give his best description of what public reason actually entails when he describes the duties that are incumbent on citizens as "they should be ready to explain the bases of their actions to one another in terms each could reasonably expect that others might endorse with their freedom and equality" (Rawls 2005[1993], 218) and "Citizens are reasonable when, viewing one another as free and equal in a system of social cooperation over generations, they are prepared to offer one another fair terms of cooperation according to what they consider the most reasonable conception of political justice; and when they agree to act on those terms, even at the cost of their own interests in particular situations, provided that other citizens also accept those terms" (Rawls 1999, 136) or, alternatively, "Public justification is

not simply valid reasoning, but argument addressed to others: it proceeds correctly from premises we accept and think others could reasonably accept to conclusions we think they could also reasonably accept" (Rawls 1999, 155).

Further, Rawls limits the scope of public reason to aspects of constitutional essentials (crucial aspects over which a society has to make decisions) and to political deliberations by citizens and especially, officers of government. While citizens, in the private deliberations or in the deliberations held by private associations, are exempt from the duty of public reason, Rawls argues that "but the ideal of public reason does hold for citizens when they engage in political advocacy in the public forum, and thus for members of political parties and for candidates in their campaigns and for other groups who support them [...] the ideal of public reason not only governs the public discourse of elections insofar as the issues involve those fundamental questions, but also how citizens are to cast their vote on these questions" (Rawls 2005[1993], 215). Alternatively, in order to hold elected officials to the duty of public reason, citizens should, in Rawls' view, think "they were legislators and ask themselves what statutes, supported by what reasons satisfying the criterion of reciprocity, they would think it most reasonable to enact" (Rawls 1999, 135).

Rawls contrasts the use of public reason with the appeal to non-public reasons, which he defines as "corporate bodies, as well as individuals, need a way of reasoning about what is to be done. This way of reasoning is public with respect to their members, but non-public with respect to political society and to citizens generally. Non-public reasons comprise the many reasons of civil society and belong to what I have called the "background culture", in contrast with the public political culture" (Rawls 2005[1993], 220). Further, in the later text, Rawls distinguishes between the background culture and the non-public political culture: "the background culture includes, then, the culture of churches and associations of all kinds, and institutions of learning at all levels, especially universities and professional schools, scientific and other societies. In addition, the non-public political culture mediates between the public political culture and the background culture. This comprises media—properly so-named—of all kinds: newspapers, reviews and magazines, television and radio, and much else" (Rawls 1999, 134n13). Thus, Rawls exempts from the requirements of public reasons the internal debates of associations, universities and professional societies, as well as media.

The exemplar of public reason is, according to Rawls, a country's supreme judiciary institution (he refers to the Supreme Court of the United States). Rawls argues that, in the case of in judicial decisions, the requirements of public reasons are strictest. He argues for this claim by quoting Ackerman's

five principles of constitutionalism and especially the distinction between the constitution as higher law and ordinary law and the claim that "a democratic constitution is a principled expression in higher law of the political ideal of a people to govern itself in a certain way. The aim of public reason is to articulate this ideal" (Rawls 2005[1993], 232). Further, Rawls describes the Supreme Court as a bulwark for the constitution in front of "transient majorities" and maintains that, unlike other institutions, public reason in the only reason that the Supreme Court exercises. Unlike citizens, who, with the exception of constitutional essentials, are allowed to vote based on their more comprehensive doctrine, the justices of the Supreme Court must "have no other reason and no other values than the political" (Rawls 2005[1993], 235). The justices, in Rawls' view, "cannot, of course, invoke their own personal morality nor the ideals and virtues of morality generally […] they must appeal to the political values they think belong to the most reasonable understanding of the public conception and its political values of justice and public reason" (Rawls 2005[1993], 236). Finally, by interpreting the constitution in a way in which all find it acceptable, the justices also give public reason "vividness and vitality in the public forum" (Rawls 2005[1993], 237).

Conclusion

The paper argued that classical literature on securitization and de-securitization privileges non-deliberative forms of contesting security. Alternatively it looks to judicial forms of de-securitization as considerably more desirable. The paper employs the concept of public reason, as developed by John Rawls could represent the key to a normatively acceptable form of contesting security.

The article analyses the literature on the normative character of securitization and agrees with those arguing in favour of the claim the securitization theory is a normative theory. Them it critiques the forms of contestation proposed in the literature and argues that these are not deliberative and that they fail to meet their own standards. Finally, the work focuses on Rawls' philosophy as a source of inspiration to argue for a public-reason inspired theory of de-securitization.

References:

1. Aradau, C., (2004), "Security and the democratic scene: desecuritization and emancipation", in *Journal of International Relations and Development* 7 (4): 388-413.

2. Balzacq, T., Léonard, Sarah, Ruzicka, Jan, (2015), 'Securitization' revisited: theory and cases, in *International Relations,* 30 (4): 494 – 531.

3. Behnke, A., (2004), "No way out: Desecuritization, emancipation and the eternal return of the political – a reply to Aradau", in *Journal of International Relations and Development* 9 (1): 62-69.

4. Buchanan, A., (1982), "Exploitation, Alienation and Injustice", in *Canadian Journal of Philosophy* 9(1): 121-139.

5. Buchanan, A., (1982), in *Marx and justice: the radical critique of liberalism* Totowa, N.J: Rowman and Littlefield.

6. Cohen, J., (2003), "Deliberation and democratic legitimacy" in Derek Matravers and John Pike (eds.), *Debates in Contemporary Political Philosophy*, London and New York: Routledge.

7. Côté, Adam, (2016), "Agents without agency: Assessing the role of the audience in securitization theory", in *Security Dialogue*, 47(6):541 – 558.

8. Floyd, R., (2007), "Towards a consequentialist evaluation of security: bringing together the Copenhagen and the Welsh Schools of security studies", in *Review of International Studies* 33 (2): 327-350.

9. Floyd, R., (2010), *Security and the Environment: Securitisation theory and US environmental security policy,* Cambridge: Cambridge University Press.

10. Floyd, R., (2011), "Can securitization theory be used in normative analysis? Towards a just securitization theory", in *Security Dialogue* 42 (4-5): 427-439.

11. Floyd, R., (2014), "Just and unjust desecuritization" in T Balzacq (ed.), *Contesting Security: Strategies and Logics*, London and New York: Routledge, 122-138.

12. Floyd, R., (2017), "Parallels with the hate speech debate: the pros and cons of criminalising harmful securitising requests", in *Review of International Studies,* http://dx.doi.org/10.1017/s0260210517000328.

13. Geras, N., (1985), "The controversy about Marx and Justice", *New Left Review* I/150.

14. Geras, N., (1992), "Bringing Marx to Justice: an addendum and Rejoinder", *New Left Review* I/195.

15. Habermas, J., (1990), "Discourse Ethics: Notes on a Program of Philosophical Justification." *Moral Consciousness and Communicative Action.* Trans. Christian Lenhart and Shierry Weber Nicholson. Cambridge: MIT Press: 43-115.

16. Lederman, S., (2014), "Agonism and Deliberation in Arendt", *Constellations* 21 (3): 327-337.

17. Mitchell, W., (1961), "Politics as the allocation of Values: a critique", *Ethics* 71(2): 79-89.

18. Rawls, J., (1999), *A theory of justice*, Cambridge Massachusets: Harvard University Press.

19. Rawls, J., (2001), *Justice as fairness: A restatement*, Cambridge Massachusets: Harvard University Press.

20. Taureck, R., (2006), "Securitization theory and securitization studies" *Journal of International Relations and Development* 9 (1): 53-61.

21. Waever, O., Buzan, B., de Wilde, J., (1998) *Security: A New Framework for Analysis*, London and Boulder, Co: Lynne Riener.

22. Wæver, O., (2011), "Politics, security, theory", *Security Dialogue* 42 (4-5): 465–480.

23. Waever, Ole, (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.

24. Wæver, O., (1998b), 'Security, Insecurity and Asecurity in the West-European Non-War Community', in Emmanuel Adler and Michael Barnett, eds., *Security Communities*, 69–118, Cambridge: Cambridge University Press.

25. Williams, Michael C., (2003), 'World, Images, Enemies: Securitisation and International Politics', *International Studies Quarterly* 47(4): 511–32.

THE ROLE OF THE MALACCA STRAIT IN THE PAST AND CURRENT REGIONAL AND INTERNATIONAL POWER RELATIONS AND SECURITY ARCHITECTURE

Mihai SANDU*

Abstract

Throughout history, one of the hottest regions in the world, South East Asia, has represented one of the highest targets for the main actors who searched for dominance on a regional or even international level. Found in the very heart of the region and of the security equations of the great powers, the South China Sea and the string of islands and straits that ensured its connections with the Indian Ocean have represented security and economic nodal points that helped spread the influence and protect the strategic interests of almost every major international player who desired to dominate the region.

Amongst these, the Malacca Strait stood and still stands today as one of the core strategic points in the region and the entire world, bringing enormous satisfaction and profits for those in control of it, while at the same time representing an increasing vulnerability for the coastal states, for the major international players and especially for the regional actors.

On a thorough analysis, controlling the Malacca Strait represented one of the main strengths for most dominant international players, either by directly controlling it or by imposing their influence on the strait through third parties or using military, political and commercial links.

Moreover, today, Malacca is one of the most important and vulnerable spots in the entire world. The high commercial and, particularly energy dependence on the strait of both regional players and international actors put Malacca in the top of the strategic points that the international security architecture depends on.

Keywords: *Malaca maritime straits, hegemony, security equations, commercial strategy, energy security.*

Introduction

History has revealed many times that a maritime power, or an actor holding a clear advantage by sea, had an upper hand when talking about

* Counselor, Parliament of Romania, mihaisandu.sandu@gmail.com.

security and power relations. Ever since the beginning of the large scale commerce by sea and the development of military sea powers, whoever controlled the seas got the chance to control or dominate commerce, particularly when talking about goods or resources mostly transported by sea.

One of the particularities of the seas regards not as much the open seas, but rather the inflexion points, the places where two or more water parts get connected, as well as those where the land and the sea make a geographical link that leaves no other option of passage.

Perhaps the most relevant examples of such inflexion points are the straits and the maritime channels, representing from the oldest times an important part of the power calculations of a state, from the primary role of blocking passage to the advantages it offered to the one in control of it due to taxes or the primary rights to resources through commerce. Of course, controlling a strait also depended on the military power, forcing the state in control to constantly increase their military power.

Found in one of the most turbulent areas in the world, the strait of Malacca represents today the most transited commercial node, with huge implications on the security and power relations and, particularly, on the energy equations. However, the importance and particularities of the Malacca strait raised it as one of the most important and relevant spots in the world from the Ancient times, with many great powers depending on it in order to impose their domination, be it regional or in the entire world.

Actors in the region in the past

The most relevant actor in the region, China`s power has always been connected to its geographic position and the advantages, as well as disadvantages it offered and has always been aware of their existence and drew their strategic games around them. From this perspective, China has attempted from the Ancient times to control and dominate on a regional perspective using key strategic points that they have identified in connection with their strategic objectives. By land, we can speak of the Silk Road and the way small Chinese communities have been established throughout Asia while by sea, China has attempted and succeeded to dominate the main maritime communication links, be it the South China Sea, the straits of Malacca and Makassar or certain islands or cities in the Indian Ocean. (Kaplan, 2014, p. 70)

Long time before the European maritime expeditions in the Indian Ocean, China has manifested, in the entire South East Asia and beyond, certain tendencies to expand its influence and create a safety area surrounding its vast empire built and maintained since Ancient times. A relevant example is that of the expeditions led by Chinese Admiral Zhang He, during the Ming

dynasty, who has organized seven expeditions in the Indian Ocean, leading fleets of over 300 ships, with carefully chosen destination points such as India, East Africa, the Red Sea, the Persian and Oman Gulfs with the strait of Hormuz between them and, obviously, the Malacca Strait and the islands surrounding it. (Harari, 2017, p. 245)

A somehow revolutionary feature of Zhang He`s expeditions for its time was the purpose and conduct of the Chinese during their visits in the places they visited between 1405 and 1433. Zhang He never attempted to conquer the ports or the regions it visited. Instead, the Chinese offered gifts, exported values and traditions, established small communities and in return, asked for the recognition of their supremacy. In other words, Zhang He`s mission was to expand the influence of the Chinese Empire on a medium to long term, creating premises for Chinese supremacy in the key points chosen and creating links that would assure a safety zone for China. (Ferguson, 2011, pp. 46-47) Everything China did through history in its surroundings and in the entire Asia is connected to such way of thinking that has been practiced since Ancient times. In case of Malacca, the communities established and the exchanges with the local populations have created an affinity that we can easily recognize today. By the time the Europeans have arrived in the region, Chinese influence was already in place and there was no way it could be reverted in such manner that would allow an opposition to China. When the Portuguese, Dutch of British colonies were established in places such as Malaysia or Indonesia, they extended the influence of the European powers in the region but could not eliminate or change the behaviour of the populations against the Chinese. Perhaps it is one of the reasons why such attempts were never relevant or even truly considered throughout history.

Due to the Chinese behaviour in the age of Zhang He and not only, by the time the Europeans arrived in the region, they came into contact with an already existing commercial, cultural and political network, facilitated by nodal points that were already in place. The Portuguese arrived first, in the 15th century, after the expeditions of Vasco da Gama and Pedro Alvarez Cabral that opened the maritime route towards the Indian Ocean and South East Asia. Their arrival in an advanced and complex market and system determined or even forced them to adapt to the models and features already in place. Taking advantage of their technological and military superiority, the Portuguese could rapidly extend their domination in the region, perhaps also taking advantage of the strategic retreat of China after the Ming dynasty was overthrown from power. In order to do so, they have conquered important cities or established new cities in key points, but mostly have imposed their domination by controlling, through intermediaries who respected their

interests, all of these being found in inflexion points or at the confluence of commercial and political networks already in place. (Paine, 2015, p. 342)

One of spots that brought about a major advantage for the competition in the area was the Malacca Strait, which ensured a connection point not just with the coastal states, but especially to the South China Sea and, perhaps most important, a bridge between the Indian and Chinese micro-universes.

Understanding the potential of the Malacca Strait, Portugal imposed and strengthened its domination over a series of commercial ports spreading from the island of Macau, through the Malacca Strait and the city of Melaka, connecting South East Asia with India, Arabia, Africa and, eventually, Lisbon. (Ferguson, 2018, p. 48) Though initially driven in the region only by the desire to impose monopoly over the spice trade, as a means to equalize the expansion of Spain in the Americas, the dynamics of the Asian trade determined Portugal to transcend from a simple player to regional hegemony. From such approach, Malacca quickly became an essential part of Portugal`s strategy, particularly due to the city of Melaka, the most prosperous seaport in the region and capital city to the Sultanate of Melaka. Apart from its strategic position that allowed domination over the passage through the strait, Melaka was also in close relationships with the Mogul Empire, which also transformed it in a passageway to the Gulf of Bengal. (Paine, 2015, pp. 348-349)

Another specificity of Melaka comes from its geographic positioning at the confluence of two large monsoon systems, the south-western one, bringing ships from the Middle East and India towards the Far East, and the north-eastern monsoon, who brought ships from the Far East towards India and the Indian subcontinent. (Kaplan, 2016, p. 104) Particularly during a time when navigation was almost exclusively performed using air and sea streams, such an advantage meant that ships were forced to go through Melaka. Such perspective not only made Melaka a strong commercial actor in the area, but also determined the creation of a cultural, ethnic and confessional mosaic that can still be observed today. Such features made Melaka an attraction point for every expanding power in the region. Chinese were there during the Ming dynasty and the Portuguese followed during their Asian expansion, both taking advantage over the fact that the Sultanate didn`t need to pursue territorial expansion policies in order to get access to resources as all were brought about by commerce. Focusing on trade, the Sultanate of Melaka`s military power was meagre, while their relationship with the Mogul Empire was not that high to ensure its security, making it an easy prey for strong expansionist actors such as Portugal in the 15th century.

Portugal quickly concretized their interest in Melaka, conquering the city in 1511 and imposing their dominion for over one and a half centuries. Melaka brought the Malacca strait in Portuguese hands as well, making

Portugal not only a major participant to the regional trade affairs, but allowed them to control some of the most important long distance routes to the detriment of their European rivals, particularly Venice. Furthermore, by getting Melaka out of the Muslim Mughal Empire`s domination, Portugal also got to control a large part of the trade between Venice and the Arabs in Alexandria, Cairo or Mecca. (Paine, 2015, p. 344)

The Portuguese conquest of the Malacca strait and the significant advantages it has offered them put Malacca definitively on top of the most desirable and important areas in the world, the strait being a part of the security equations and power relations between the major actors ever since. Over the next years, Portugal started to benefit even more from their rule over Malacca. As all the spices came through Malacca, reaching the Arabs in Mecca and, afterwards, heading towards Cairo through the Gulf of Aden and the Hormuz Strait, Portugal got to impose their domination over the entire route, controlling, in part, the entire trade in spices.

It was specifically due to this set of advantages that the Strait of Malacca drew the attention of the Dutch Empire, who became the world hegemony after the decline of Portugal following the Spanish conquest in 1580. The Dutch reach Malacca around 1595, focusing on the conquest and establishment of what later became Indonesia, turning it into an alternative to the Indies, controlled by Great Britain. Indonesia quickly becomes the Dutch trade centre in the region, with Batavia (today`s Jakarta) hosting the headquarters of the Dutch East Indies Company. (Neguț, 2009, p. 53)

Through Indonesia, the Dutch controlled the Malacca Strait and gained priority access to the Strait of Makassar, South China Sea, Java Sea, the Moluccas Sea as well as the multiple archipelagos in the area.

The first joint stock company in history, the Dutch East Indies Company got to rapidly extend and consolidate their monopoly in the region, by practicing trade on a global scale. Due to the capitalist system promoted by the Dutch East Indies Company, the huge profits encouraged and attracted large investments, which were mainly directed in extending and modernizing the Dutch commercial and military fleet, which got to stabilize the Dutch dominion. (Ferguson, 2018, p. 38)

In the meantime, the British Empire got in control over India and the British East Indies Company got to rival the Dutch one in the Indian Ocean trade map. Eventually, following a series of agreements between the two companies and between the Dutch and British Empires, the two sides split the market into the trade with spices, through Malacca, under Dutch monopoly, and the trade with Indian textiles, under British rule. (Ferguson, 2018, p. 42)

It is one of the particular reasons for why the British are not interested in Malacca at first, prioritizing their control over India and allowing the Dutch

to dominate the strait and the region. However, due to this agreement and the monopoly over the trade in textiles, the British forced the Dutch to forward them a significant share of the trade with China, becoming a *de facto* beneficiary of the trade between China and India. Their dominion has been extended after the Opium Wars, determined by the Chinese dependence on the drug coming exclusively from India that opened the large scale trade between China and the Great Britain and significantly extended the British influence in the region. (Gombrich, 2006, pp. 264-265)

In time, the British Empire became more interested in Malacca, as their influence grew worldwide while Dutch Empire was in decline. But the most important moment happened in 1819, with the creation of the city-state of Singapore, after an agreement between Great Britain, the East Indies Company and the Sultanate of Johor. Using Chinese colonists, the British forged the new state on western values and models in the best positioned spot in the Malacca Strait and in the very heart of Malaysia. Later, in the 20th century, following the collapse of their Colonial Empire, the British tried to maintain their power in Singapore with the aid of a local governance of western orientation. The British plan concretized with the rise to power of Chinese lawyer Lee Kuan Yew. Benefitting from British education, Lee succeeded in quickly transforming Singapore into one of the most prosperous states in the region, but also into a stability and balancing factor in the region, in one of the most relevant examples of *soft power*. Maintaining the connections with Great Britain at the highest possible level, Lee managed to assure a trade connection between China and Europe, while at the same time forging an alliance with Malaysia and avoiding both the Chinese direct domination and the regional power ambitions of Indonesia under the rule of Dictator Sukarno. (Kaplan, 2016, pp. 134-137)

A new and remarkable turning point for the situation of the Malacca Strait happens in 1972, when Indonesia proposes a pact to the two other coastal states in the strait that implied the three states taking over control over the strait. The pact was nothing else than another attempt of Indonesia to impose as regional power and front state in the Non-Aligned Movement. Lee Kuan Yew categorically refuses, militating for maintaining the strait as an open international maritime way and understanding the exceptional role it played in the international trade and strategic system. It is the moment when Lee`s conduct proves the effects and benefits of the American hegemony installed in the international system after World War II – the so-called *Pax Americana*. Understanding the importance of keeping the United States as close as possible, Lee argued that the Non-Aligned Movement existed in the respective region due to the Americans` fight against communist regimes that allowed non-communist states to develop under the

protective umbrella of the United States in the world. Using such an argument, Lee admits not just the existence of US interests in the Malacca strait and surroundings, but also expresses the desire of Singapore to get closer ties with the giant in the West. (Kaplan, 2016, pp. 142-143)

Lee`s approach towards the United States did not refer only to the attitude of Sukarno, but was particularly determined by the need to get some assurances in case of a more assertive position of China, the biggest power in the region and the second most powerful communist regime at the time. The fear of China was not at all random and not just because of the geographical closeness or of the commercial and geopolitical equations of China. Rather, it was due to the Chinese populations in the area that Lee tried to force an approach that would keep them away from China`s sphere of influence.

Given the strategic retreat after the Ming dynasty, China`s presence in the entire South East Asia was almost eminently carried on by the Chinese communities established in certain areas who continue to influence even today through their traditional connections with other Chinese communities. In South East Asia and particularly in the Malacca Strait region, Chinese have not just represented a link between almost every state or city in the region, but also one of the intermediaries that have facilitated trade inside and outside the regional frame. The great commercial links and international partnerships were established using the Chinese minority as bonding, an ethnic line that basically assured the connection between Singapore and Honk Kong or between Thailand and Malaysia, despite the latter having the characteristic of a real ethnic mosaic. (Landes, 2013, p. 399)

At the end of the 18th and beginning of the 19th centuries, the Strait of Malacca was not just a crossroads for trade and geopolitical networks, nor was it only a small mosaic of local populations. In time, Portuguese, Dutch, British, as well as Chinese or Indians – all had passed through, temporarily imposed their domination and, eventually, had installed their long term presence either through colonies established and developed, such as Singapore for Great Britain or Indonesia for the Dutch, or through merchants` and colonists` districts in major cities such as Manila, Batavia or Melaka. Of all, except on the case of Singapore who was maintained as a city-state under British protectorate, the Chinese had the most resilient way to impose their domination or control over the region, one that did not necessarily involve a direct conquest. Either by entering the administrative or economic structures of several countries in the region, at a local or general level, or by imposing itself as an internal arbitrator to their local issues, Chinese have created or determined the creation of structures and networks similar to the ones in China or even directly dependent to them. (Paine, 2015, p. 406)

In the 18th century, throughout the entire South East Asia there are Chinese communities, often self-administrated, coexisting with Europeans` presence in certain areas such as Melaka, the sultanate of Johor or in the Dutch East Indies, as Indonesia used to be named at the time. This hasn`t allowed only the perpetuation of a direct contact and a means for the Chinese Empire to influence the states in the region, but also an increase of contacts and commercial cooperation, laying the foundations for today`s commercial mosaic that we can see in the region. (Kerr, 2015, p. 55)

The network China created in the region not only resisted and still exists today, but also represented a basis from which China has launched itself in its influence extending strategy on a regional and global level that we can also see today.

Actors in the region in the present

Nowadays, the Strait of Malacca is an integrated part of what is likely to be the main commercial and strategic node in the world. Together with the neighbouring straits of Sunda, Lombok and Makassar, as well as the South China Sea and the other small insular seas, Malacca forms the connection between the Indian and Pacific Oceans, bringing different worlds together. The region is transited by over half of the world trade every year, one third of the total maritime traffic and, in energy concerns, two thirds of the supplies for South Korea, around 60% of the supplies for Japan and Taiwan and approximately 80% of the necessary raw oil for China. (Kaplan, 2014, p. 26)

The worldwide high dependence on Malacca that we see today makes it vulnerable not just in regard to economic and commercial exchanges, but also in what concerns piracy, terrorism and organized crime, particularly in the ports. Today, the most crowded commercial node in the world does not benefit from an international cooperation frame that would include not just littoral states, but also regional powers and international actors. Today, littoral states are forced to rely mostly on their own resources and capabilities, with very little aid from other states in what concerns the development of such capabilities. (Arsyad, 2008, p. 176)

Of course, Chinese dependence on the energy imports coming through Malacca is not a matter of novelty. However, the constant raise of this dependence and the increase in the energy commercial volume transiting Malacca has the tendency of becoming problematic, furthermore in the context of China not having realistic serious alternatives to it, while the littoral states, particularly Indonesia and Malaysia, manifest constant development and economic growth that might put them in an increasingly stronger position in relation to China.

As an answer to this, China has been continuously extending its influence not just in the South China Sea, but through the entire South East Asia, basically using two relevant methods: strategic expansion, through the control upon certain strategic points from where it could exert its influence – the so called "String of Pearls" with which China has been attempting for years to control certain nods or spots that would extend their position at a regional and world level; and the construction of artificial islands in the South China Sea through which it could expand the territorial waters under its jurisdiction and where it could easily unfold operations of exploration and exploitation of oil and gases in the continental shelf.

The latter represents a tactic used by China in its attempt to somehow dodge the international law and conventions in the field, particularly the United Nations Convention on the Law of the sea, according to which China shares exclusive maritime economic areas with Indonesia, Taiwan or South Korea. (Christensen, 2015, p. 98)

The construction of artificial islands does not represent the only tactic adopted by the Chinese in the South China Sea. There currently are a large number of inhabited islands of very small dimensions that China seeks to control including by artificially extending their surface. The most well-known and relevant examples are those of Spratly and Parcel Archipelagos, disputed over with the Philippines and Vietnam and where China currently leads a dynamic expansion policy by extending its control over the territorial waters of these islands and by strategically placing oil platforms in the area. At least in these two cases, China takes advantage over the silent standing aside by the international community, and particularly by the United States of America, who, in general, do not intervene in litigious situations regarding disputed islands, insisting instead on a peaceful resolution of such litigations, in conformity with international law and in a way that would not trouble the freedom of navigation. (Christensen, 2015, p. 102)

In the context of the Malacca Strait, one simple look at the map reveals that, with the extension of its control over the territorial waters through the Spratly Archipelago, China gets closer enough to the mouth of Malacca. Logically, one may ask what will be the next step of China should its intentions in Spratly and Parcel be successful. Will China attempt a dispute with Singapore, Malaysia or Indonesia over some of the main small islands at the Eastern border of Malacca that Beijing would afterwards use to control, together with Singapore, the Eastern mouth of the strait and thus reverse China`s dependence on Malacca?

China`s expansion in the South China Sea isn`t, however, the only relevant example of strategic orientation and increasing tendency in its search

for solutions that would reduce their Malacca dilemma. Today, the access to the Malacca Strait increasingly becomes one of the strategic sources for China, particularly in regard to its access to energy resources. In fact, China has been trying for years to multiply diversify their sources for energy. For example, by taking control of the Gwadar port in Pakistan, while in the meantime massively investing in rebuilding the ancient Silk Road and other such land routes, China increasingly reduces its huge dependency of the straits of Malacca of Hormuz, overcrowded and largely controlled today by USA and its allies. (Chomsky, 2015, p. 85)

But how can China extend its influence in or around the Malacca Strait following the example of the Gwadar port? How and when would China be able to activate their historic "marks" applied throughout the region by developing commercial networks and, particularly, by establishing and supporting local Chinese communities in other countries or by maintaining the strategic dependence connections with smaller countries they had created over centuries?

Further, one the main issue regards the world rivalry between China and the United States of America. For years, the US have been considering China as an expanding hegemonic power that requires a balancing that the American Administration needs to perform basically through regional allies. On the other side, China regards the actions of the United States as part of a large scale containment plan with the purpose of stopping the legitimate rise of China. Both visions fit into the dynamics of power balance in the most realist terms, fact officially demonstrated by the US-ASIA Rebalancing Strategy that President Barrack Obama has launched in 2011 and by the Counter-Intervention Strategy of China. If we add to the two strategies the East Asia Pivot of the Russian Federation and India`s Look East Policy, the regional scenery gets more and more complicated, like a multiple chessboard where the US moves with its 7th Fleet and China counters with the fast militarization of South China Sea, while every actor in the region tries to draw advantages through strategic control over parts of the commercial nod that includes the Strait of Malacca. (Sharma, 2014, p. 255)

In what concerns the United States of America, the main purpose of President Obama`s strategy was to create a constant naval military pressure upon the chain of straits Malacca-Sunda-Lombok-Makassar, as a coercive strategy that would moderate China`s behaviour and eventually force it to remain within the first island chain, formed by the main archipelagos along the East Asian coast. (Sharma, 2014, p. 256)

Without leaving their *Asian Pivot*, the most recent US National Security Strategy adopted by President Donald Trump in December 2017 includes

fewer specific references to South East Asia. Their support for regional allies remains high, as does the objective of a more articulated presence in the region. Besides, however, except on an intensified economic rivalry, the strategy and policy of Donald Trump manifests a high ambiguity, for now, in what concerns this region. Of course, Trump`s rhetoric remains aggressive enough, but we currently don`t have enough reliable data that would help us strategically comparing today` US intentions with those of the USA under the Obama administrations. (*National Security Strategy of the United States of America*, December 2017) Can we speak of a shift in US policies? As has already been proved in the mandate of the current US President, not shifts seem to be the issue, but rather a high degree of unpredictability that US presence on the international level less clear and sometimes even surprising. Given the well-known obsessions of Donald Trump in regard to China, it is highly unlikely that the US today won`t grant enough attention to Beijing or to its regional and international ambitions. Furthermore, Trump`s policies and rhetoric regarding a possible resolution of the North Korean file brings US on a new chapter in South East Asia, one that hasn`t involved Washington DC for quite a while.

As a response, China not only continues its strategic rhetoric concerning South East Asia, but also considers West Pacific as a vital zone for its own sovereignty, integrity, security and development, seeking to identify strategic locations, strategic resources and strategic domination, completing their *String of Pearls*. Complementary, China tries to impose a long-distance domination in the Indian Ocean-West Pacific region through their "Far Seas Ocean Strategy". (Sharma, 2014, p. 258)

Clear enough, both powers will continue to hold and strengthen their influence in South East Asia and particularly in the area of the Malacca Strait. In the meantime, India`s sphere of influence is expected to be maintained and even extended as well, considering their regional ambitions that many times stand against the Chinese ones.

Conclusion

Of course, the most important actors will remain the three coastal states, Malaysia, Singapore and Indonesia, all three considered for the past decades as part of the emerging countries, due to their economic boom, the high rate of investments, their social developments and their increasingly important and relevant geopolitical power. On every possible scale, their opening to the Malacca Strait will continue to be their main advantage as well as vulnerability, furthermore as China`s dynamic and almost aggressive

expansion in the South China Sea undoubtedly regards Malacca as a possible target if not an objective.

In the meantime, Malacca will remain and even consolidate its position as the most overcrowded commercial node in the world, continuing to represent an advantage as well as vulnerability for most actors involved. Its uniqueness and the traditional geographical position it has will continue to make Malacca, as well as the other straits and small seas in the region, an active player in the security and power equations in the region and, without a doubt, in the entire world.

References:

1. Arsyad, Rosihan, (2008), "Cooperation to Safeguard Shipping through the Malacca Strait", Andrew Forbes (Ed.), *Asian Security: Regional Cooperation in the Malacca Strait*, Canberra, Sea Power Centre – Australia.

2. Chomsky, Noam, (2015), *Because we say so*, Great Britain, Hamish Hamilton.

3. Christensen, Thomas J., (2015), *China ca provocare,* Bucharest: Comunicare.ro

4. Ferguson, Niall, (2011), *Civilizația. Vestul și Restul*, Iași, Polirom.

5. Ferguson, Niall, (2018), *Imperiul*. *Cum a creat Marea Britanie lumea modern*, Iași, Polirom.

6. Gombrich, Ernst H., (2006), *Istoria Lumii*, Bucharest, Ed. Pro-Editura, 2006.

7. Harari, Yuval Noah, (2017), *Sapiens. Scurtă istorie a omenirii,* Iași, Ed. Polirom.

8. Kaplan, Robert D., (2014), *Răzbunarea Geografiei*, Bucharest, Ed. Litera.

9. Kaplan, Robert D., (2016), *Marea Chinei de Sud și sfârșitul stabilității în Pacific*, Bucharest, Ed. Litera.

10. Kerr, Gordon, (2015), *O scurtă istorie a Chinei*, Pitești, Ed. Nomina.

11. Landes, David S., (2013), *Avuția și sărăcia națiunilor*, Iași, Polirom.

12. *National Security Strategy of the United States of America* (Washington DC: December 2017), at https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

13. Neguț, Silviu, (2009), *Introducere în Geopolitică*, Bucharest, Ed. Meteor Press.

14. Paine, Lincoln, (2015), *Marea și civilizația*. *O istorie maritimă a lumii*, Iași, Ed. Polirom.

15. Sharma, Balkrishan K. Maj.Gen. (Ret.), (2014), "Asia-Pacific Security Challenges. Trends and Implications", *A Collection of Papers for the 2nd International Conference on Security and Cooperation in the Asia-Pacific Region*, China Institute for International Strategic Studies, Beijing.

THE REFUGEE CRISIS AND HOW IT IMPACTED THE EUROPEAN CONTINENT

Mircea ORMENIŞAN*

Abstract

In order to understand this crisis, there is a need to look back at what triggered this with the main catalyst being the Syrian civil war. It can be said that the incident started once with the Arab Spring protests back in 2011 as the Syrian population grew in discontent with the Bashar al-Assad government resulting in protests in hopes of removing said government. Sadly the protests were violently suppressed and sparked the fire of armed conflict in the country, throwing it in the civil war that has ravaged the country.

The purpose of this article is to shed some light on the current refugee crisis that the European Union is facing, especially on the negative aspects of it that came under the form of a surge in criminal activity and terrorist acts, how it affects the Union, its security and the security of its citizens.

Keywords: *refugee crisis, crime rate, criminality, terrorism, crime.*

Introduction

In order to understand this crisis, there is a need to look back at what triggered this. The main catalyst of the crisis was the Syrian civil war. It can be said that the incident started once with the Arab Spring protests back in 2011 as the Syrian population grew in discontent with the Bashar al-Assad government resulting in protests and hopes of removing said government. Sadly the protests were violently suppressed and sparked the fire of armed conflict in the country, throwing it in the civil war that has ravaged the country.

As the violence in Syria escalated, millions fled their home in order to seek refuge or find a better life, with Al-Jazeera estimating that around 11 million had fled the country or that they had been displaced as of 2015 (Al

*University of History and Philosophy Babes Bolyai, Security Studies English Line, E-mail: ormenisanmircea1@gmail.com.

Jazeera, March, 2015). However the first Syrian refugee to touch the shores of Europe was registered in 2012 and by 2015 more than 313000 asylum applications were filed Europe, with Hungary being the first to be overburdened by the applications and refusing to accept any more refugees, a decision that sparked great controversy. Because of the great influx of refugees, Germany and the Czech Republic had to suspend the Dublin Regulation (a EU law that determines the EU Member State responsible for examining an application for asylum seekers seeking international protection under the Geneva Convention and the EU Qualification Directive, within the European Union (Council Regulation (EC) No 343/2003), with the objective to prevent an applicant from submitting applications in multiple Member States and to reduce the number of "orbiting" asylum seekers, who are shuttled from member state to member state with the country in which the asylum seeker first applies for asylum is responsible for either accepting or rejecting the claim, and the seeker may not restart the process in another jurisdiction) for Syrians and started to manually process the applications, followed shortly by a plan to redistribute 120.000 asylum seekers across the EU, drafted and accepted by ministers of interior and home affairs of the EU. The plan was rejected by mostly East European countries, some speculating that economic and social cost would prove too much of a strain for them.

How refugee crisis impacted the European continent

By 2016 Austria imposed a restriction on the number of refugee entries, Slovenia and countries of the Balkan region announcing that they will allow a number of 580 refugees per day to pass their borders, putting a serious strain on the Greek authorities that are stuck with large numbers of refugees on their hands, sparking fears that the Greek government will not be able to handle this situation and may prove dangerous for their internal security.

Looking at statistics and numbers, Austria had 18.000 Syrian refugee arrivals in 2015; by 2018 the number reached 48.103 only for Syrian nationals. The Czech Republic on the other hand was accused of breaking human rights for the “degrading conditions in which the refugees are held, some claiming this is a tactic to deter refugees from remaining in the country (Migrant Crisis: Czechs Accused of Human Rights Abuses – BBC News, 2015). France even though after the Paris attacks of 2015 had remained stern on its decision to accept more than 30.000 refugees, as Francoise Hollande stated that it is France’s humanitarian duty and “we have to reinforce our borders while remaining true to our values” (The Washington Post, 2015). Germany

had received around 12.000 refugees of Syrian origin in the year of 2013, with the number more than tripling by 2014 (39.332) and by 2015 reaching around 161.000. It is important to note that after the suspension of the Dublin Regulation, the influx of refugees had started to seriously stress German infrastructure and logistics. Germany at the moment has the highest approval of asylum requests at 96%, authorities expecting more to come (BAMF – Bundesamt Für Migration Und Flüchtlinge, December 2015).

Hungary however is at the complete other side of the spectrum since 2015 it has closed its border and erected a fence with barbed wire on the southern borders, especially with Croatia and it blocked train travel. The government itself sees the refugees as illegal immigrants that seek jobs and a danger the Hungarian culture and proceeded to outlaw refugees and reject asylum claims at the border (The Guardian, September 15, 2015). Poland, as well, had a stern approach towards the refugee crisis as it accepted only 150 refugees mostly of Christian beliefs and as the population had shown strong anti-migration and anti-refugee sentiments and after many polls had demanded a stop to refugee quotas.

Romania was asked to house around 6.500 refugees according to EU quotas, but the Romanian government negotiated that it will accept this only if EU will grant its citizens equal access to the visa-free Schengen area.

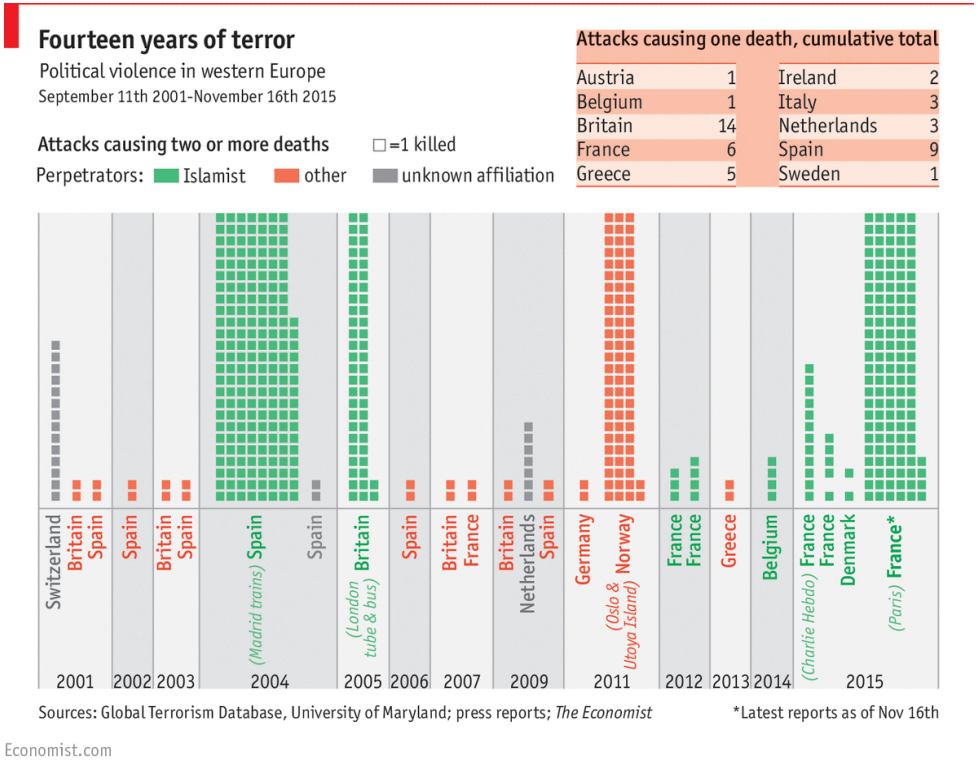
Sweden was the first country in the EU that granted permanent residency to all asylum seekers as well as the right to reunite with their families (more exactly to bring them to Sweden). As of 2012 almost 3.000 Syrian nationals settled in Sweden as refugees, grew to more than 9.000 in 2013 and doubled in 2014 summing up to approximately 31.000 refugees with an additional 9.000 that settled on the grounds of family reunification. Sweden received 10.000 stateless individuals on the grounds of them residing previously in Syria. As of 2015 51.338 Syrian refugees had applied for asylum in Sweden but after 2015 the number of applications has decreased (Asylsökande till Sverige 2000-2017). As a critique, there have been concerns that these policies may be a launch pad for a boom in the people smuggling business.

Please note that the numbers and statistics are for Syrian refugees only and do not include those from Afghanistan, Iraq, Eritrea, Libya and so on.

As the saying goes each coin has two sides, and the EU's open border policies also brought disastrous events under the form of terror attacks and a spike in crime rates, the most affected by it being France and Germany.

As it is known, France has went through one of the most shocking and horrific episodes from its history during the November 2015 attacks in Paris, were a series of well-coordinated terrorist attacks occurred: suicide bombers struck at the Stade de France during a football match, followed by mass shootings and suicide bombings at a number of cafés and restaurants and one of the more notorious mass shooting occurring at the Bataclan theatre. Thanks to the professionalism and quick reaction of the French authorities, the further escalation of these incidents was cut short.

Table 1: Attacks that had caused at least one death
(September 11th 2001 – November 16th 2015)
(Source: The Economist, November 16, 2015)



With the table above (The Economist, November 16, 2015), one can observe that in the past 14 years, Europe has been affected by a wave of terrorist attacks made by Islamist perpetrators, with the year 2015 mostly

affecting France with the Charlie Hebdo and November attacks. The acts of Friday 13th claimed 129 lives; the shootings at the office of the satirical magazine Charlie Hebdo, the beheading of a man at a chemical plant near Lyon as well as a foiled armed attack on a TGV train are part of the incidents that have impacted the French population. It is important to focus on one key piece of evidence that came up after the investigations of the 2015 attacks as a supposed Syrian passport was found near the lifeless body of one of the perpetrators, which bore the name of Syrian national that transited through Greece earlier in October. The passport eventually proved to be fake and the credentials on it were that of a loyalist soldier of Bashar al-Assad that had died months ago before the incident, the rest of the assailants being identified EU nationals and it is believed that they had been radicalized by Islamic State operatives from the Middle East or it has been a homegrown radicalization (The Washington Post, 2015). The incident itself sparks debates and concerns, the possibility of radical Islamists infiltrating the continent might prove in fact to be a reality. With the EU opening its arms towards refugees it is complete ignorance or stubbornness to not admit the fact that this will eventually bring unwanted outcomes. The fact that the borders are so open towards refugees or even if they would become more restricted in the future is still a good prospect for illegal activities as human trafficking might boom, with a good example being the rise of cocaine prices in the US post 9/11, as well as people being the new commodity that cartels smuggled in country, as it proved more beneficial for them since it meant that they didn't have to grow or produce it (which implicated time in the equation for illegal profit), only needing to charge the individuals that wished to cross the border. The same scenario can be applied to Europe today, Sweden's policy of offering permanent residency for asylum seekers might even encourage people smuggling, or even the prospect of a more closed border could still boom this illegal activity as tight borders are good for business.

Table 2: GTD, terrorist attacks ranked by fatalities in Europe (2001-2018) (Source: GTD Search Results, 2018)

GTD ID	DATE	COUNTRY	CITY	PERPETRATOR GROUP	FATALITIES	INJURED	TARGET TYPE
201511130008	2015-11-13	France	Paris	Islamic State of Iraq and the Levant (ISIL)	93	217	Business,Private Citizens & Property
201607140001	2016-07-14	France	Nice	Jihadi-inspired extremists	87	433	Private Citizens & Property,Private Citizens & Property
200403110003	2004-03-11	Spain	Madrid	Al-Qaida (suspected)	73	450	Transportation,Transportation
201107220011	2011-07-22	Norway	Utoya	Right-wing extremists	69	60	Private Citizens & Property
201605190058	2016-05-19	Greece	Unknown	Unknown	66	0	Airports and Aircraft,Private Citizens & Property
200403110007	2004-03-11	Spain	Madrid	Al-Qaida (suspected)	62	450	Transportation,Transportation
200403110001	2004-03-11	Spain	Madrid	Al-Qaida (suspected)	37	450	Transportation,Transportation
200507070002	2005-07-07	United Kingdom	London	Al-Qaida	27	340	Transportation
201705220006	2017-05-22	United Kingdom	Manchester	Islamic State of Iraq and the Levant (ISIL)	23	119	Business,Private Citizens & Property,Private Citizens & Property
201511130006	2015-11-13	France	Paris	Islamic State of Iraq and the Levant (ISIL)	19	26	Business,Private Citizens & Property
200403110004	2004-03-11	Spain	Madrid	Al-Qaida (suspected)	19	450	Transportation,Transportation
201603220001	2016-03-22	Belgium	Zaventem	Islamic State of Iraq and the Levant (ISIL)	18	135	Airports and Aircraft,Private Citizens & Property
201603220002	2016-03-22	Belgium	Brussels	Islamic State of Iraq and the Levant (ISIL)	17	135	Transportation,Private Citizens & Property
201511130003	2015-11-13	France	Paris	Islamic State of Iraq and the Levant (ISIL)	15	26	Business,Private Citizens & Property
201708170002	2017-08-17	Spain	Barcelona	Muslim extremists	14	101	Private Citizens & Property
200507070004	2005-07-07	United Kingdom	London	Al-Qaida	14	110	Transportation
200109270003	2001-09-27	Switzerland	Zug	Unknown	14	18	Government (General)
201612190002	2016-12-19	Germany	Berlin	Jihadi-inspired extremists	12	48	Private Citizens & Property,Private Citizens & Property
201501070001	2015-01-07	France	Paris	Al-Qaida in the Arabian Peninsula (AQAP)	12	12	Journalists & Media,Police,Private Citizens & Property
201706030010	2017-06-03	United Kingdom	London	Jihadi-inspired extremists	11	48	Private Citizens & Property,Private Citizens & Property

In the table from above there is a list of incidents (the only parameters set for the search was the European Continent, a time period from 2001 up to 2018 and the list was ordered by number of fatalities the incident had produced) that had happen in the span of 17 years, all ordered by the number of fatalities each had produced (GTD Search Results, 2018). One can easily observe that the majority of the perpetrators were affiliated with a radical Islamist movement and the incidents seem that a surge in these attacks had occurred since the Syrian refugee crisis had begun. It can be seen that France has faced most of them, followed by the United Kingdom, but fatalities are not the only thing to worry about as in Germany the police reports for 2016 were presented (PKS: Gewaltkriminalität Steigt in 2016 Dramatisch – Schelmenstreich), there was an increase in rapes and murders done by refugees, more specifically 12% of the murders and 14,9% of rapes were committed by refugees (which make roughly 3% of the population). (Bericht Zur Polizeilichen Kriminalstatistik, 2016)

Conclusions

As a conclusion, one can realize that the refugee crisis can have a devastating outcome for the European continent and the Western Values that it holds, proving that the mass importing of refugees has become a burden for most European countries as their National Security Services are lacking personnel. Along with the overcrowding of the security infrastructure had proven to be critical for the success for Islamic terrorist cells or radicals to infiltrate and establish a base of operation. A solution could be that each European citizen should consider enlisting in one of their National Security Services, especially the younger generations since there is a need for young and motivated individuals with a strong will to serve in such services because a youth with a strong sense of duty and a population with a security culture will make almost impossible the possibility of an escalation in terrorism. The future of next generations lays solely in our hands, it is our duty to stay united, to stay strong and to stay vigilant in the face of evil.

References:

1. "What's Left of Syria?", Al Jazeera, March, 20-15. Accessed October 7, 2018. https://www.aljazeera.com/indepth/interactive/2015/03/left-syria-150317133753354.html.

2. "Council Regulation (EC) No 343/2003." Accessed October 8, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003R0343&from=EN.

3. "Migrant Crisis: Czechs Accused of Human Rights Abuses - BBC News." Accessed October 7, 2018. https://www.bbc.com/news/world-europe-34604118.

4. Were Syrian refugees involved in the Paris attacks? What we know and don't know", The Washington Post, 2015. Accessed October 7, 2018. https://www.washingtonpost.com/gdpr-consent/?destination=%2fnews% 2fworldviews%2fwp%2f2015%2f11%2f18%2ffrance-says-it-will-take-30000-syrian-refugees-while-u-s-republicans-would-turn-them-away%2f%3fnoredirect%3don%26utm_term%3d.0e7047b22b0a&noredirect=on&utm_term=.0e7047b22b0a.

5. "BAMF – Bundesamt Für Migration Und Flüchtlinge – Downloads Und Publikationen – Asylgeschäftsbericht 12/2015." Accessed October 7, 2018. https://www.bamf.de/SharedDocs/Anlagen/DE/Downloads/Infothek/Statistik/Asyl/201512-statistik-anlage-asyl-geschaeftsbericht.html?nn=1364454.

6. "Refugee Crisis: Hungary Rejects All Asylum Requests Made at Border – as It Happened. World News, The Guardian, September, 2015. Accessed October 7, 2018. https://www.theguardian.com/world/live/2015/sep/15/refugee-crisis-hungary-launches-border-crackdown-live-updates.

7. "Asylsökande till Sverige 2000-2017," n.d.

8. "Terror Attacks and Arrests in Western Europe. Daily Chart, The Economist, November 16, 2015. Accessed October 7, 2018. https://www.economist.com/graphic-detail/2015/11/16/terror-attacks-and-arrests-in-western-europe.

9. "GTD Search Results", 2018. Accessed October 7, 2018. https://www.start.umd.edu/gtd/search/Results.aspx.

10. "PKS: Gewaltkriminalität Steigt in 2016 Dramatisch - Schelmenstreich." Accessed October 9, 2018. http://schelmenstreich.de/polizeiliche-kriminalitaets-statistik-pks-2016-gewaltkriminalitaet-steigt-dramatisch/.

11. "Bericht Zur Polizeilichen Kriminalstatistik", 2016. Accessed October 9, 2018. http://schelmenstreich.de/wp-content/uploads/2017/04/pks2016ImkBericht.pdf.

ULTIMATE CAUSES OF WARS (LONG-TERM, STRATEGIC CAUSES) AND DIFFERING ROLES FOR INTELLIGENCE PRACTITIONERS, ACADEMICS, AND POLICY MAKERS

Michael ANDREGG*

Abstract

Promoting constructive relations between academics and intelligence practitioners in the US is a perennial challenge. Many centripetal forces drive us apart. This challenge will be illustrated by reference to four of the most important ultimate causes of wars and crises that all civilizations face today. Those long-term causes of conflict are: 1) Population Pressure; 2) Corruptions of Governance; 3) Militant Religion, and 4) Authoritarian Law.

That conclusion followed review of over 400 relevant books, structured interviews with over 100 long-term (>20 years' service) accomplished, military, intelligence and diplomatic personnel, and a similar number of long-term, accomplished peace advocates. This resulted in a book that won our National Peace Writing Award in 1999. (Andregg, 1997, 1999, 2001) The concept of a 'developing global crisis' (DGC) that underlies more proximate (more visible, & often less controversial) causes of wars has been presented at many military and intelligence colleges since then, where officers often struggle with the differences between strategic and tactical intelligence. Very few people want to get into unending wars, but militaries lean towards tactics. We reply that medicine teaches us that to cure grave problems one must identify ultimate causes, not deal just with symptoms.

Population Pressure is an ultimate (strategic) cause of wars well illustrated by contemporary Syria, by displacement of Native peoples in North and South America by European immigrants, and by many other examples. However, no US politician speaks about this openly due partly to opposition from organized religious groups. So our military is now trapped in wars that never end in places with high birth rates and endemic violence like Afghanistan and Iraq. Many try to promote "moderate" (non-violent) forms of Islam there. But our partners are often assassinated by terrorists who reject modernity, and who see collaboration with foreign occupiers as treason.

* University of St. Thomas in St. Paul, MN, USA, mmandregg@stthomas.edu

Corruptions of Governance obstruct solutions to big problems everywhere. Academics are well informed about those, which makes us irritating. Intelligence professionals are usually employed by governments, as are policy makers, which make criticizing governments difficult for them. So academic critics of policy are often seen as nags or worse, and the scholars are frustrated by being ignored or even actively opposed by bureaucracies that resist change fiercely.

Militant Religion and Authoritarian Law interact synergistically, which complicates everything. This combination drives terrorist enthusiasm for violent "solutions" to the many problems they seek to overcome by ruling the entire world. Thus, "Caliphate" has become a label for militant, religious authoritarianism. I will tie each of these factors to implications for both practitioners and policy makers, despite their long-term and very problematic political implications.

Keywords: *causes of wars, intelligence practitioners, academics, and policy makers.*

Introduction to a simplistic Matrix

Theorists try to simplify even hyper-complex problems to better understand and discuss them. Therefore, I provide the very simplistic matrix below as a framework from which to discuss how these four major forces interact with the different job categories or roles we often find ourselves in. To emphasize our common goal, I quote America's recently retired top intelligence officer, former Director of National Intelligence and Air Force General James Clapper. "Factors like **food and water shortages** and poor living conditions – increasingly driven by **climate change** – **oppression** of political freedoms, **corruption** by **autocratic** governments and rulers who had been in place for decades – … made them (failed states) extremely unstable." (Clapper and Brown, 2018) The only ultimate cause that Clapper does not mention in this one sentence is militant religion, but there are plenty of comments on that in his discussions of the apparently endless "war on terrorism."

A. Matrix of ultimate causes of wars by job categories of responders

NB: "IP's" means Intelligence Professionals, or Practitioners in this matrix.

	Practitioners	**Academics**	**Policy Makers (PMs)**
Population Pressure (PP)	Cannot affect PP, and work time dominated by short-term crises.	Can study for decades (and have) producing clues for solutions.	Must try to reconcile taboos on discussion **and** deal with mainly short-term crises.
Corruptions of Governance	Employed by Gov'ts, exposing corruption is very risky for IP's.	We love studying corruptions, often with no practical solutions.	PMs have to live, and secure real power, in corrosive environments.
Militant 'Religions'	Faced with huge #'s of unemployed, male, desperate, militarized radicals.	My 'practical' solution requires taboo violation which is risky for most. ('good vs. bad' religion)	Policy should support the 'good' spirituals, while defeating 'bad' religious terrorists.
Authoritarian Law (AL)	IP's internal order is paramilitary, but external problems **require** human rights.	'We' hate AL so much that many find it very hard to collaborate with IP's constructively.	Many PMs dream becoming 'dear leaders' if not a God's dictators with impunity.

Presume for the moment that there is neither doubt nor controversy over the proposition that population pressure is a powerful, ultimate cause of wars and other problems. The point here is to observe how different job types interact with that. First, intelligence practitioners are besieged daily with often time-urgent problems of tactical kinds. They have very little free time, and zero ability to do anything short-term about population issues. They also are almost never asked to attend to long-term issues by their taskers, and may even be punished for venturing into "policy." Academics, on another hand, have decades to ponder ultimate causes of conflicts and to work on potential solutions to those, relatively free from political constraints. Most policy

makers (in my experience) are fairly well aware of population issues, but seldom speak about them and almost never publicly, because they must survive intensely political environments, which can (and often do) reject and replace them if they dare to discuss taboos in public. Why population issues are politically taboo is a topic for another day, but every practical politician is familiar with that and why the taboos exist. Political opportunists exploit this factor by raising legitimate fears of immigration, then exaggerating these by demonization of ethnic or religious minorities.

Some large fraction of the endemic conflicts that seldom end in Africa and the Middle East, for example, are driven by these kinds of "tribal politics." They are also driven by high birth rates. (Andregg, 2018) But it is much easier to talk about political and religious differences, about relevant histories and personalities of key leaders, than about the underlying tectonic force of high birth rates, which lead to population pressure, resulting in endemic wars and occasional genocides. That dynamic is almost never mentioned by people who want to keep their jobs in politics or even in academe.

We asked readers to "presume that there is neither doubt nor controversy over the proposition that population pressure is a powerful, ultimate cause of wars and other problems" knowing that there is much doubt and inevitable controversy over that proposition. Nazli Choucri and Robert C. North proved it in 1975, but their work failed to gain traction due to the pervasive opposition to thinking about high birth rates as a cause of conflicts. (Choucri and North, 1975) Therefore, we will spend some space on proving that proposition now. For the other three proposed "ultimate" causes of wars and genocides (Corruptions of Governance, Militant Religion, and Authoritarian Law) we will focus on implications for practitioners, academics and policy makers, rather than writing another book.

Evidence that population pressure is an ultimate cause of wars and genocides

The case of the disintegration of Syria from 2011 to the present day is particularly vivid and has more reliable metrics than many, so we will concentrate on that case here, then on historic genocides of North and South America. But there are many other historic examples, from Easter Island to World War II to the expulsion by force of Rohingya from contemporary Myanmar. (Blomquist, 2016; Blomquist and Cincotta, April 12, 2016) The danger is spending so much time on proving the importance of any factor that one loses focus on how differently academics, practitioners and policy makers must deal with such factors.

In 2010, the population growth rate in Syria was 2.4% per year. (CIA World Factbook, 2010) This leads to a doubling time of just under 30 years and a highly "pyramidal" age distribution with many more young than elders. In addition, the worst drought in Syria's recorded history occurred during the four years prior, leading to migration of at least 1.5 million (of Syria's then 22 million people) from barren farmlands into overburdened cities. ("A Syrian Refugee at COP21," by Andrea Liverani, 21 October, 2015) Climate change contributed to that drought, and global warming is a substantial and significant consequence of the global increase in human populations and especially in consumption of fossil fuels. It is a derivative result of population pressure.

Syrian conflicts began with simple protests of largely students in Damascus, who sought a fairer distribution of job opportunities from the government of Bashar al-Assad. He was reserving the best for his Alawite ethno-religious group, with some for minority Christians in a predominantly Sunni country. He followed in his father's footsteps by crushing protests, which introduces those other ultimate forces of corruptions of governance and authoritarian law. But this time, the tidal force of population pressure combined with militant religion, which was growing throughout the region. So, despite many casualties, protests endured, became more militant and better armed, and morphed over a few years into a hyper-complex and brutal series of civil wars. This led to over half a million dead, half of the pre-war Syrian population displaced, and at least 6 million refugees who fled to near neighbors (1 million went on to Europe) spreading population pressure to all those areas, but especially to fragile Jordan and Lebanon, and increasingly militant Turkey. (*UN High Commissioner for Refugees, 29 August, 2015*) Meanwhile, the Alawite population in Syria grew from 11% in 2010 to about 17% in 2014. (CIA World Factbook, 2014)

Moving back in time, we note quickly that "*Lebensraum*" (living room) was a powerful theme in Hitler's excuses for invading his neighbors. Population pressure was also long seen in Japan as the primary reason for invading China first, then many Southeast Asian nations and Pacific islands. In fact, the Japanese Diet (Parliament equivalent) publicly debated the need to feed another million Japanese babies every year, and the impossibility of doing that on the resources of their largely mountainous island nation. Thus, real and imagined concerns about dire needs to secure the resources of weaker neighbors were a powerful force in the genesis of World War II.

The innumerable small wars in North and South America, and occasional outright genocides, provide some equally compelling numbers. For one example, the land on which my Universities stand and the entire territory

of Minnesota was 99% Native American "Indians" in the year 1800. By 1900, one short century later, the state of Minnesota was 99% whites of European ancestry, with only ½ % Native Americans. The remaining ½% was blacks who left the South after our own Civil War. ("Turn of the Century: Minnesota's Population in 1900 and Today") There was a seminal point, now called the US – Dakota War of 1862, when the native Lakota and Dakota Sioux were forcibly expelled to far away, barren territories. Bounties were even offered by our first Governor for scalps of Indian heads, a dramatic contrast to contemporary values and laws. Along with the Sioux, many Ojibwe, Ho-chunk, Winnebago, and other native tribes suffered and died, or moved to mainly remote and desolate areas.

This is actually a story as old as human history, and enumerating examples can take lifetimes. The lesson of Easter Island is especially instructive, because it was another island civilization that destroyed itself and its supporting ecosystem. From a high of 20,000 people on a 14 by 21 kilometer island with normal wood and other resources, they killed each other and deforested their island until when Captain Cook found it in 1774, there were only about 1,000 remaining. Novel diseases further decimated them, to a low of 114 survivors. More examples and technical analysis is found in Chapter 12 of the previously cited book on the causes of wars, pp. 62-73. (Causes of War, pp. 62-73, 2001) But talking about population pressure still remains quite difficult for academics and politicians.

Of course, there are contrary cases as well. For example, Russia has no intrinsic need for more land today. Its population growth rate is currently negative, and its residual empire occupies the largest area of any modern nation. (CIA World Factbook, 2018)[1] But President Putin misses the glories of the old Soviet Union, and his drive for power and wealth knows no limit. So today, Putin rules one of the most corrupt and authoritarian regimes on earth. They routinely assassinate critics and competitors to maintain Putin's rule and oligarch wealth. Hybrid warfare destabilized Ukraine. Putin seized Crimea at a vulnerable moment with "little green men," ("Annexation of Crimea by the Russian Federation") and maintains military forces in other "frozen conflicts" in Georgia and Moldova to this day. Population pressure is not a cause of those conflicts, rather corruptions of governance and Putin's affection for authoritarian law.

[1] Sections on Russian geography and demographics: Russia currently occupies 17,098,242 square km, and their growth rate in 2017 was negative .08% per year.

Corruptions of governance

Virtually every adult with a brain recognizes that corruptions of governance are a powerful cause of wars and many other problems. Corruptions of governance also obstruct solution to problems, even when practical solutions are easily apparent to scientific and economic communities (as with climate change, or controlling inflation). However, law enforcement in general and intelligence agencies in particular face some immediate dilemmas that complicate effective action in support of their overall noble mission, which is protecting the peoples of nation states.

First, all involved are employed by governments, which make looking at local corruption risky. Gathering data on corruptions in adversary governments is often OK, and some intelligence professionals specialize in information operations employing such tradecraft.[2] Russian "active measures" have always included this dimension,[3] and they have raised exploiting corruptions in other governments (and people) to an art form. But criticize their own government? The price in Russia is often death, with especially gruesome deaths for defectors from the security services.[4]

Second, noble police and armed forces are undoubtedly focused on protecting both states and people. However, their dangerous work, centuries of history, and the priorities of paymasters make each group more casual about "collateral damage" (a.k.a. murder of innocents) than most citizens are. Since states control definitions of terms like 'murder' and create euphemisms like 'collateral damage' to cover their own sins, it is quite hard for practitioners to ignore the obvious desire of governments to avoid

[2] Two very instructive cases are Peru under Alberto Fujimori, who was indicted after videos appeared showing his intelligence chief Vladimiro Montesinos bribing Congressmen, and Turkey's Recep Tayyip Erdogan who went after the followers of an ex-patriate Imam named Fethullah Gulen who revealed corruptions at the top of Turkey. Both cases are hideously complicated, so I simply note these examples of information operations of great consequence that were focused on exposing corruptions at the top of nominal democracies.

[3] "Active Measures" is the most important and well-credentialed documentary yet produced on Russian efforts to disrupt the 2016 US elections. It was produced by Jack Bryan and released on Hulu on 31, August 2018.

[4] The murder by polonium 210 poisoning of KGB defector Alexander Litvinenko in London on 1 November, 2006, is a type case of this kind of retaliation against Russian intelligence veterans, because the cause and the poisoners are known, and the manner of death was very slow, gruesome, visible and incurable. The more recent attempt to poison double agent Sergei Skripal and his daughter Yulia with novichok nerve agent in Britain on 4 March, 2018 is another. There are, unfortunately, many other such cases where precise causes and participants are less well known.

accountability for crimes that they cause. Most involved on that side of the power equation prefer impunity for their acts of violence and other crimes.

So, basically, many academics are decades ahead of many practitioners and policy makers on perceiving corruptions of governments, understanding their dynamics, and formulating possible solutions for both the big problems, and for the smaller but intense dilemmas that practitioners and conscientious policy makers face when their chain of command goes bad.[5] This happens much more often than professors of intelligence studies tend to admit. Pity the good German Generals who recognized that Hitler's madness would destroy their great nation. Thousands were killed when their attempts to assassinate him failed. ("Assassination Plot against Hitler Fails") And pity whistleblowers from America's intelligence community today who try to reveal waste, fraud or abuse within their systems, much less wrongdoings that led to million-death "mistakes." [6]

You do not hear much about national security whistleblowers from police states like Russia, China or a long list of other nations we wish not to offend, because they are often killed or imprisoned so efficiently that their stories never make it to polite society. Intelligence practitioners are keenly

---

[5] The most obvious example of solutions for insider moral dilemmas is whistleblower protection legislation. In the USA, most federal employees enjoy such protection from punishment for revealing waste, fraud and abuse – excepting specifically intelligence employees. Therefore, associations of retired IC members who support whistleblowers now exist, including VIPS (Veteran Intelligence Professionals for Sanity) and a related National Security Whistleblowers Coalition, see https://en.wikipedia.org/wiki/National_Security_Whistleblowers_Coalition.

[6] The best example of this from recent times was fraudulent intelligence presented to promote the second invasion of Iraq by US forces in March 2003. This is a very complicated example where there were plenty of simple mistakes and groupthink. But there were also examples of crudely forged documents, and fraudulent testimony of unverified "sources" in foreign countries that were more than just mistakes. The ultimate proof was failure to find any of the Weapons of Mass Destruction that were alleged to "certainly" exist in Iraq. Detailed reviews can be found in A Pretext for War: 9/11, Iraq, and the Abuse of America's Intelligence Agencies, by James Bamford, New York, NY: Anchor Books, division of Random House, 2005, and The Greatest Story Ever Sold: the Decline and Fall of Truth in Bush's America, by Frank Rich, New York, NY: Penguin Books, 2006. Retaliation against US government employees in this affair is also well documented in "Fair Game," both a book and a documentary about CIA veteran Valerie Plame Wilson and her diplomat husband Joseph. A review of these open sources combined with some secret (i.e. IC) sources was presented by this author at the Fifth "Need to Know" conference in Greifswald, Germany on 6 November, 2015 titled "The US Decision to Invade Iraq in March, 2003, Chasing Phantom WMDs: How Human Intelligence was Used, Abused and Politicized to 'fix the facts around the policy,'" accessible at: https://static1.squarespace.com/static/5750629760b5e9d6697be6cd/t/59dcd32651a58476eab47044/1507644200230/Need+to+Know+V+Greifswald+dfinal.pdf .

aware of this consequence for looking into corruption of their police states, so even most conscientious practitioners look in some other direction. Lord knows, there are plenty of other threats to the state one can attend to, like real terrorists and organized crime. Corrupted intelligence services lose their loyalty to citizens, and often conclude that students, teachers and grandmothers protesting grievous wrongs are criminals or even "terrorists." Police states are especially prone to equating peaceful protest with treason, or at least criminal riot, and they routinely label patriotic government whistleblowers as traitors to the state. Democracies are not immune to these perverse transformations of common language and traditional justice.

The history of intelligence "whistleblowers" in America is discouraging. Daniel Ellsberg became a national name when he shared Pentagon documents with major media that revealed years of government lying about the war in Vietnam. They threatened him with prison and possibly death, until a rare judge declared that whistleblowers are true patriots.[7] A most recent example, Reality Winner, was sentenced on 23 August, 2018 to over five years in prison for revealing one NSA document on Russian meddling in the 2016 US elections. (Holpuch, 23 August, 2018) Before her, Edward Snowden achieved unwanted fame by revealing to our public and the world that the US government was routinely scanning most domestic telephone and many email communications in violation of our Constitution. Before him, Thomas Drake from the NSA was persecuted for discussing the same hard truths (a story stranger than fiction described on "60 Minutes").[8] Before him Army private Chelsea (a.k.a. Bradley) Manning was sentenced to 35 years in prison for revealing unpleasant truths about our war in Iraq. (New York Times, 21 August, 2013) In each case, unusually conscientious intelligence professionals chose their oath to protect and defend our Constitution over contracts with US government agencies to keep all secrets no matter how severe, immoral or even illegal. Most were punished more severely than financial criminals who steal billions and injure millions.

---

[7] Daniel Ellsberg was prosecuted under the 1917 Espionage Act, which stipulates the death penalty in extremis. Fortunately for Ellsberg, a judge dismissed the charges two years later because Ellsberg was not a foreign spy, but rather a patriot trying to alert our country about grievous wrongs planned in secret and lied about for many years. This dichotomy of "patriotic whistleblowers" vs. "treasonous secret leakers" is peculiar to democracies.

[8] The "60 Minutes" story of Thomas Drake can be found at: https://www.youtube.com/watch?v=_mVpMp9QLPE. A later interview with Drake for "Frontline" is archived at: https://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-thomas-drake/

This puts a big strain on the consciences of many real patriots who make careers in intelligence, the military and law enforcement, especially when corruptions of high office become as blatant, egregious, and as damaging to true national security as we observe in 2018. But there is little relief for insiders unless other groups create "political space" for dissent among employees of the state. Even then, revelations from the professional military are fraught with danger. Moral dilemmas faced by policy makers are similar, and profound. They must succeed in toxic moral environments that make it very difficult for truly honest and good men or women to succeed.

One of our sources who achieved high office in an allied intelligence system pointed out that 80% of his work time had to be devoted to fending off efforts from domestic competitors for his job. This is more than just workload; it is one reason they all have armed security details. That is when the top leaders are relatively democratic and 'clean.' The dilemmas faced by patriots in decaying police states are rather more severe. My country is facing a very hard test today of the "checks and balances" created by the writers of our Constitution to deal with such high-level corruption. We currently endure the most corrupt President in living memory who is also acting like an asset of a foreign adversary, with thousands of nuclear weapons under his command. At the time of writing, anything could happen from impeachment to World War III.

Lord Acton's most famous quote is relevant here: "Power corrupts, and absolute power corrupts absolutely." Acton has a much less famous comment for intelligence practitioners, judges and policy makers, which were: "***Everything secret degenerates, even the administration of justice; nothing is safe that does not show how it can bear discussion and publicity."*** (Gasquet and Abbott, 1906)

Therefore, in sum I conclude that the lion's share of work on exposing government corruptions and proposing solutions must remain with the journalists and academics who have chosen that task aware of how many are imprisoned or even killed each year for their efforts to improve and secure the peoples of their nations. But I also educate policy makers and intelligence practitioners about this problem often, because their information cocoons can be so pervasive that some forget that our citizens are not 'the enemy' unless we are traitors to national values.

Militant 'Religion'

One key to decoding this extremely problematic, ultimate cause of many wars and genocides lies in the definition of 'religion' and more cogently, on discerning fundamental differences between "good" religions

and "bad" religions. Therefore, a few words on that never-ending landmine are relevant here.

First, one can observe that even the scripture-based "religions of the book" display a spectrum from peace oriented, life-affirming, community building practices and people who try hard to elevate everyone to better health, wealth, and spiritual enlightenment, to a much darker group who truly believe that their 'god' loves them much more than any other persons. Those claim that their interpretation of religion or divine revelation is the only accurate version, and in the most extreme cases, that destiny desires them to rule the entire earth, often by violent means.

This spectrum is not limited to people who make religions of words, however allegedly perfect. Even gentle Buddhism can produce both gentle Buddhists and militant religionists who urge war against non-believers, as in the civil war in Sri Lanka from 23 July, 1983 to 17 May, 2009, and the expulsion of Muslim Rohingya by militant Buddhist armies in contemporary Myanmar.

Wishing to focus on how this difficult, strategic cause of wars affects the worlds of practitioners, policy-makers and academics, I submit an observation on the genesis of this odd phenomenon of religions animating both peacemaking and warmongering behaviors. The fundamentalist, and so often militant, end of the spectrum displays behaviors indistinguishable from the selfish genes of modern evolution theory. The spiritual, life-affirming end of this spectrum displays behaviors urged by all the prophets and often modeled by exemplary lives of service to all humankind. Those folks feed the hungry and heal the sick. The militants plot for power and commit crimes. People come in both kinds. And both may use "religion" as inspiration for their behaviors.

For policy makers, one practical result is that it is generally OK to point out the evil behaviors of "terrorists" in enemy camps, and even to detail how militant versions of <u>their</u> religion inspire and instruct them. If one points out that there are equally cruel members of the home religion, the power of the policy maker may disappear overnight, if indeed they survive the night.

Intelligence practitioners do more of their work in secrecy, so they have a bit more latitude, and every analyst with a brain recognizes that militant 'religion' is a cause of many problems today. But they still work in fairly authoritarian government groups. So if the boss is a member of a militant clan (or cult) their job can still be at risk. Whatever their position, intelligence agencies are notoriously prone to "politicization" of their

estimates, conclusions and recommendations. Therefore, this is a conundrum worth contemplating for conscientious intelligence professionals.

Once again, academics in non-police states are freer to comment bluntly on this factor, even on the similarities between militant religious groups and destructive cults.[9] Therefore, I can say what practical politicians almost never do, that "religions" come in both good and bad varieties. One is life affirming, constructive, healthy, and often inspired by 'revelation' or spiritual figures including some called prophets. The other is not life affirming, but rather is selfish and arguably "Darwinian." The latter also tends to be much more vocal about its "religion." Since the militants are much more violent than authentic spirituals, they tend to dominate if not wipe those out.[10]

One practical aspect deserves comment for the intelligence professionals among us. Religious extremists often suppress women and express strong commitments to having large families. I have seen advertisements in their literature about this as a tactic of war, or to prevail in political competitions against their less zealous religious competitors. Thus, militant religion also tends to support high birth rates, another of the most powerful ultimate causes of wars and genocides. And thus, we are faced today with tens of millions of often poorly educated, barely employable teen-aged males with little hope for families much less healthy futures. Such men are easy to hire by demagogues who use "religion" as a cover for crass political greed of every kind. This also points to solutions, like strong encouragement of education for women, modernization of tribal codes and gender roles, and easy access to things like modern contraception despite predictable resistance

[9] Research on destructive cults, fundamentalist religions and connections between those and "mainstream" religions is extensive, so we will cite just four books here. Margaret Thaler Singer wrote Cults in our Midst: The Hidden Menace in our Everyday Lives, with Janja Lalich, published by Jossey-Bass Publishers of San Francisco, CA, in 1995. The Roots of Evil: The Origins of Genocide and other Group Violence, was written by Ervin Staub in 1989, and published by Cambridge University Press. Enemies of Freedom: Understanding Right-wing Authoritarianism, was published by Jossey Bass in San Francisco, and won the AAAS award for best Social Science research in 1988 for its author, Bob Altemeyer. Finally, perhaps the most extensive review of fundamentalist religions and their relations with other religions was published by the University of Chicago Press in 1991 as part of a long-term project. Its 888-page magnum opus was edited by Martin E. Marty and R. Scott Appleby, titled Fundamentalisms Observed. This paradox of peaceful religions animating violent behaviours was so perplexing to this author that I camped with a group called the Christian Patriots Defence League at their freedom festival for three days in 1979, surrounded by armed militia who were protecting us from ... someone. I learned a great many things about this topic there, but since they are neither published nor easily reproducible, I will spare readers details here.

[10] The crucifixion of Jesus of Nazareth can be cited as one example of a pacifist killed by militant competitors.

from the most militant wings of whatever religions prevail in that region. "They" want many obedient soldiers, with few options for making a viable life doing productive things.

Militant "religions" provide moral cover for the brutal activities of wars and genocides.[11] However, without actual, practical power, they will not prevail. Authoritarian Law provides the money, equipment, training, and legal justifications for large scale, organized armed conflict by states. Thus, the two factors in combination are much more dangerous than either one alone. Therefore, we turn now to Authoritarian Law.

Authoritarian law

Everyone recognizes that an American President (or a Russian President) could order a massive, nuclear attack against hundreds of cities half a world away at any time, resulting in probable destruction of civilization itself in the northern hemisphere. Such is the logic of "Mutual Assured Destruction," commonly known as MAD. It is less obvious, but no less true, that this capability is entirely dependent on authoritarian law.

First, is the chain of command, supported by vast recruitment, training, legal and educational foundations that teach millions of sworn officers and enlisted personnel that it is their solemn duty to obey the "Commander in Chief" no matter what. [12]

Second it comes the vast amounts of money expended over decades or even generations required to actually build thousands of nuclear warheads and their associated delivery systems. That money is not acquired by persuasion, but rather by laws backed by force that compel citizens to pay taxes for security purposes no matter what they feel about how their financial support is used.

Finally, third comes judiciary systems that reinforce the coercion of soldiers to obey, and citizens to support state violence regardless of personal

[11] ISIS, or "Islamic State," which is ironically neither authentically Islamic nor a state by any definition, provides the most graphic examples today of this paradox of militant 'religion' inspiring brutally cruel behaviours. There are many historic examples, but I do not want to irritate my neighbors with reference to "Manifest Destiny" or "Crusades."

[12] We could digress here to discuss the much weaker guidelines for U.S. officers and troops to resist, or even to disobey "unlawful orders." Any such order to fire nuclear weapons at targets under great time pressure, if properly authenticated, would likely be considered lawful, and our nuclear forces have refined their techniques to weed out anyone who might let conscience override training in a crisis. We are confident the Russians have trained and selected their nuclear troops to obey also. Thus, Authoritarian Law can become more powerful than pacific religion.

conscience. This is why protestors of state violence are commonly jailed, while perpetrators of state violence very seldom are. The judges and the laws are integral parts of authoritarian systems. Extended over generations, one result is a culture of authoritarian law that fundamentally supports state violence over international peace, or even human rights at home, which are often abandoned during declared emergencies.

Of course, governments vary a lot in their degrees of authoritarianism. Those differences are quite important, which is why I comment often on differences between police states and more enlightened governments. Virtually none exemplify the "Golden Rule," which is mentioned in the scriptures of every written religion and in the principles of native peoples worldwide. [13]

Bob Altemeyer of Canada won the 1988 American Association for the Advancement of Science (AAAS) award for best work in Social Science that year by suggesting that authoritarian law is one byproduct of a personality trait. This work was preceded by a great deal of intense study of similar themes after the Nazi debacle in Europe, animated by the question of how or why so many "Good Germans" could become faithful followers of a madman who ultimately destroyed their own country along with many tens of millions of other victims. (Arendt, 1963, 1977, 2006; Adorno et. al. 1950) Altemeyer's work was followed by hundreds of studies in political psychology and sociology that cited him. [14]

But our purpose here is probing how Authoritarian Law affects intelligence practitioners, policy makers, and academics. The first point to observe is that most intelligence practitioners work in authoritarian systems where obedience to some chain of command is the most highly prized virtue. By number, the most work in military intelligence organizations where strict obedience to mission and command has been reinforced by centuries of combat that show how important unity of command is. Yet even "civilian"

[13] Native peoples, of course, can also be warlike and have been thousands of times in human history. We are not trying to be romantic here, just note that the same spectrum from life affirming, and humanity building spirituality to barbaric, warmongering savagery exists in every population we have seen so far. A deeper analysis suggests that this spectrum exists in the behavioural repertoire of normal human beings, who are products of evolutionary histories that put premiums on survival and reproduction, both of individuals and of the small (often tribal) groups they tend to associate with. Thousands of years of history including hundreds of genocides reinforce this behavioural template.

[14] Also noteworthy were classic experiments by Stanley Milgram (Obedience to Authority, 1974) and Philip Zimbardo (The Stanford Prison Experiment, 1971) but we digress into political psychology again.

agencies (like the CIA in America) often operate like paramilitary organizations in terms of their command and control, rewards and punishments, and specialized rules of duty to their agency more than to their country, much less to citizens. [15]

Working every day in authoritarian organizations that control paychecks and pensions as well as mundane things like definitions of *duty, justice, freedom, legal, criminal* and other words with big consequences makes it very difficult for insiders to dissent in any meaningful way. And yet most of the really great problems on our earth require considerable respect for concepts like human rights, rule of law, and definitions of "justice" that are remarkably different from those used by police states. One might note for example the differences between such terms in the Romania of Nicolae Ceaușescu, as compared with any of its successor governments no matter their inevitable flaws. Like people, every government has feet of clay too, but the spectrum from better to worse is extremely important to both world security and human survival.

As usual, the academics have more freedom, but much less power to do anything significant. That challenge is compounded by the fact that many academics are viscerally opposed to authoritarian law in all its forms, often because they have been repressed in the past or because they have spent lifetimes studying repression and corruption among authoritarian systems.

This culture gap often makes it hard for academics and intelligence practitioners to work well together even when both sincerely want to. Key words have different meanings, so we often talk past each other. One group's devotion to secrecy and one-way information flows clashes with the other's devotion to free exchange of information, and constant testing of hypotheses against evidence from world-wide networks. Questions of 'loyal to who or what' loom over every interaction, and trust in the basic humanity, good will and honesty of collaborators is fragile.

That makes constructive collaboration difficult, sometimes exhausting, and occasionally dangerous. Many academics fear that any known connection to intelligence agencies will ruin their reputation among strictly academic colleagues. And some intelligence professionals are so afraid their precious secrets will leak that they seldom or never take the risks of collaboration.

---

[15] As illustrated by the severe punishments applied to U.S. national security whistleblowers when compared with the many other sins committed by intelligence personnel, much less politicians. We all have feet of clay, but resistance to the god of authoritarian law is undoubtedly punished much more aggressively in the USA than most of our human transgressions.

Fortunately, enough intelligence professionals graduate to become professors at universities, and enough academics have family in security services to know that they do not eat babies every day.

Policy makers are in the delicate position of transcending such boundaries. Many are extremely dependent on secret information from professional intelligence services, so they obey the rules of secrecy, but they work (at least in theory) for the citizens of their nations. Whatever their political inclinations, they usually sincerely want to do the best they can for their countries and for *most* of the citizens of those countries. The special problem policy makers' face is that most are politicians of one sort or another. And like politicians everywhere, their most common secret dream is to become Commander in Chief of the Universe. Darwin talks to all of us.

Conclusions

The ultimate strategic challenge of our time is between civilization and barbarism, or in fact, between life and death for billions of people. The outcome is in doubt, and there is not infinite time to solve these great problems. Therefore, I urge every intelligence practitioner, academic, policy maker and hybrids thereof to do their best to both act on immediate crises effectively, and to develop the global vision and wisdom necessary to keep strategic challenges in mind.

For example, waves of migration from poor and violent areas toward richer and safer countries will continue for the foreseeable future. And even if they could be walled off perfectly by some imaginary structure or technology, the problems of failed states would fester until disease or WMDs find their way across borders. We must deal with ultimate causes, not just symptoms, and we must be global, not just local. Stopping excess migrants is dealing with a symptom only. Population Pressure, violence, and Corruptions of Governance are ultimate causes of migration.

Climate change is a tidal force that will keep pressure boiling in areas closer to the equator. And global warming is entirely a derivative consequence of relentless population pressure. Substantial solutions to those issues are well within the grasp of modern technology, if politicians would allow the engineers and biologists to do what they know is necessary, humanely, carefully, but expeditiously, before sea level rise puts every coastal region at risk and wars spread everywhere.

Corruptions of governance (and other institutions) frustrate solutions worldwide. The IT revolution makes exposing corruptions ever easier, but that same revolution also empowers police states today, as witness the plight

of the Uyghur people in Northwest China. Beijing is deploying facial recognition cameras everywhere there, and authoritarian police and intelligence forces with the best of artificial intelligence use 24/7 surveillance technologies to identify any trace of critical thought or resistance in the Xinjiang Uyghur "Autonomous" Region. (Denyer, 7 January, 2018) China's plan to develop social obedience scores for every citizen is beyond even Orwell's imagination.[16]

Repression often works for a while … until it fails with catastrophic consequences as it did in Syria. Dozens of Chinese Emperors died because of that dynamic; you would think they would learn from their thousands of years of history. The same can be said for militant religion. No matter how barbaric, states founded on that principle always fall in the end because their zealous dogmas repel, imprison, or even kill the creative people who invent great things and build new businesses. When the cranks and critics are allowed to be different, some will create a Google.[17]

I claimed that time for solutions are not infinite. For example, Pakistan is a country in turmoil today. How long will it be before a Pakistani (or a North Korean) nuclear warhead finds its way to Islamic extremists elsewhere who are committed to delivering one to Tel Aviv? (Hoodbhoy, Pervez and Mian, August, 2018) Or two for Washington D.C. and Moscow simultaneously? How many other great cities would go up in flames elsewhere after such trigger events? No one knows, but I know that we must deal with root causes and very delicate strategic conundrums, because managing symptoms is not enough.

Nightmare scenarios are easy to conjure; solutions to great problems are considerably harder to achieve. But I have confidence in the intelligence of intelligence agencies (if not always of their wisdom). And I know that policy makers have children too, who depend upon us all to find real solutions that endure, even if that places some strain on careers.

It is also easy to find historic examples that support a theory, but accurate prediction is the ultimate test. Therefore, I will be a fool and venture a prediction that is easily testable. The current U.S. President is so remarkably

---

[16] George Orwell is best known for two books that presented authoritarian law in its most lethal end state, the police state. These were 1984 (published in 1950) and Animal Farm (published in 1984, by Houghton Mifflin, NY).

[17] Co-founder of Google and now President of Alphabet, Sergey Mikhaylovich Brin was born, ironically in Moscow, Russia on 21 August, 1973 and is now worth ~ 54.5 billion dollars. Creative people like Brin employ tens or even hundreds of thousands of people, and create new wealth in many ways. Crushing creativity is counterproductive.

corrupt and narcissistic that he will be prone to starting a foreign war (or wars) to distract attention from his domestic critics.[18]

The greatest danger of this will start near the date of the 24th IKS Conference (October, 2018) and extend through any moves to impeach Mr. Trump. The most likely targets are 1) Iran, and 2) North Korea, because they are both relatively small countries, much less powerful than the USA and far away. Venezuela is another possible target, but less likely for many reasons. Within one year, readers can know if this prediction of attacking a scapegoat to further Trump's political ambitions is correct or not. However, if he starts a war to distract discontent, it will not be because of population pressure in America (which is minimal) or militant religion. It will be because of profound corruptions of governance and Trump's deep affection for authoritarian law.

The strategic challenge of our time is between civilization and barbarism. We must heal the living system that supports us all, and stop destroying it by endless wars over petty, tribal, dominance issues. Civilization is life affirming (like authentic spirituality) while barbarism is not, and self-destructs where it dominates. Civilization took thousands of years to create; it is worth preserving and enhancing. Do your best to pass it on to our young.

Academics, practitioners and policy makers all have slightly different roles in the epic challenge of our time. I am confident readers will rise to that challenge if we are indeed professionals and patriots, dedicated to the security of our states and of the people in them.

References:

1. "A Syrian Refugee at COP21," by Andrea Liverani, 21 October, 2015, accessible at: http://blogs.worldbank.org/peoplemove/syrian-refugee-cop21.

2. "Annexation of Crimea by the Russian Federation," Wikipedia entry, accessible at: https://en.wikipedia.org/wiki/Annexation_of_Crimea_by_the_ Russian_ Federation

3. A Pretext for War: 9/11, Iraq, and the Abuse of America's Intelligence Agencies, by James Bamford, New York, NY: Anchor Books, division of Random House, 2005.

4. Andregg, Michael, (1997, 1999, and 2001), *On the Causes of War*, St. Paul, MN: Ground Zero Minnesota Center for the Study of Intelligence and Wisdom.

[18] This form of scapegoating is sometimes called Simmel Effect after Austrian Georg Simmel who wrote about it in "The Sociology of Conflict," in American Journal of Sociology, IX, pgs. 490-525, 672-689 & 798-811, 1903-1904.

5. Andregg, Michael, (2018), "Birth Rates Determine Life Expectancy in Theoretical Equilibrium Populations: Implications for Political Demography and Conflict Early Warning," in the American Intelligence Journal, Vol. 35, no. 2.

6. Arendt, Hannah, Eichmann in Jerusalem: A Report on the Banality of Evil, New York, NY: Penguin Books, 1963, 1977, 2006, and Adorno, T.W., E. Frenkel-Brunswik, D.J. Levinson, and R.N. Sanford, The Authoritarian Personality, New York, NY: Harper, 1950. See also Bob Altemeyer's Enemies of Freedom, cited in endnote #26.

7. "Assassination Plot Against Hitler Fails," on "History.com" at: https://www.history.com/this-day-in-history/assassination-plot-against-hitler-fails.

8. Blomquist, Rachel, (2016), "Ethno-Demographic Dynamics of the Rohingya-Buddhist Conflict," in the Georgetown Journal of Asian Affairs, Fall, pp: 94-117. This is accessible at: https://asianstudies.georgetown.edu/sites/asianstudies/files/documents/gjaa_3.1_blomquist_0.pdf.

9. Blomquist, Rachel, Cincotta, Richard, (2016), "Myanmar's Democratic Deficit: Demography and the Rohingya Dilemma" in New Security Beat, Wilson Center's Environmental Change and Security Program, April 12, at: https://www.newsecuritybeat.org/2016/04/myanmars-democratic-deficit-demography-rohingya-dilemma/

10. Clapper, James, Troy Brown, (2018), *Facts and Fears: Hard Truths from a Life in Intelligence*, New York, NY: Viking Books.

11. Choucri, Nazli, North, Robert C., (1975), *Nations in Conflict*, San Francisco, CA: Freeman.

12. CIA World Factbook, 2010, section on Syrian demographics.

13. CIA World Factbook, 2014, section on Syrian demographics.

14. CIA World Factbook, 2018, sections on Russian geography and demographics, accessible at: https://www.cia.gov/library/publications/the-world-factbook/geos/rs.html. Russia currently occupies 17,098,242 square km, and their growth rate in 2017 was negative .08% per year.

15. Denyer, Simon, "China's Watchful Eye," in the Washington Post, 7 January, 2018, is accessible at:
https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/?undefined=&utm_term=.2e073329aec5&wpisrc=nl_headlines&wpmm=1.

16. Gasquet, Abbott, Lord Acton and his Circle. New York, NY: Longmans, Green, 1906.

17. Hoodbhoy, Pervez and Zia Mian, "Managing Pakistan's Bomb: Learning on the Job," in the Bulletin of the Atomic Scientists, August, 2018, at: https://thebulletin.org/2018/08/managing-pakistans-bomb-learning-on-the-job/.

18. Holpuch, Amanda, "Reality Winner: NSA Contractor Jailed for Five Years over Classified Report Leak," in The Guardian (US News Edition) 23 August, 2018, at: https://www.theguardian.com/us-news/2018/aug/23/reality-winner-sentence-classified-report-leak?utm_source=esp&utm_medium=Email&utm_campaign=GU+Today+USA+-+Collections+2017&utm_term=284128&subid=18936390&CMP=GT_US_collection.

19. "Manning Sentenced to 35 Years for a Pivotal Leak of U.S. Files," in the New York Times, 21 August, 2013, accessible at: https://www.nytimes.com/2013/08/22/us/manning-sentenced-for-leaking-government-secrets.html.

20. The Greatest Story Ever Sold: the Decline and Fall of Truth in Bush's America, by Frank Rich, New York, NY: Penguin Books, 2006.

21. The "60 Minutes" story of Thomas Drake can be found at: https://www.youtube.com/watch?v=_mVpMp9QLPE. A later interview with Drake for "Frontline" is archived at: https://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-thomas-drake/.

22. This form of scapegoating is sometimes called Simmel Effect after Austrian Georg Simmel who wrote about it in "The Sociology of Conflict," in American Journal of Sociology, IX, pgs. 490-525, 672-689 & 798-811, 1903-1904.

23. "Turn of the Century: Minnesota's Population in 1900 and Today," a publication of the Minnesota Planning State Demographic Center, editor Martha McMurray, especially page 7, November, 1999.

24. *UNHCR Syria Regional Refugee Response/Total Persons of Concern". UN High Commissioner for Refugees, 29 August, 2015.*

A FAUSTIAN PACT: THE REGIME OF TRUTH WITHIN NATIONAL SECURITY DOCUMENTS IN ROMANIA AND GERMANY

Iulian DICULESCU-BLEBEA*

Abstract

The main purpose here is to open an academic door towards a very inciting and promising nexus, to launch an invitation to scholarly "occupy" the common niche of truth and security – which appear to become increasingly relevant, especially against the background of the currently re-emerging ideas and debates around post-, hybrid-, fake- and many others alike. This study focuses on how the idea of (a crisis of) the regime of truth is addressed, as a whole or through some of its core elements, in a series of strategic documents. It investigates whether and how it is framed as a matter of security, showing the official approaches in which the Romanian and German authorities frame and tackle the problem in the particular instances given by their respective security strategies. The hermeneutical approach of these documents, based on a Foucauldian conceptual toolbox and his archaeological approach for the „questioning of the document", with accent on their specific perceptions and understandings, on their actual and latent content, indicates how and in what a surprisingly extensive manner these strategies address issues related to the core elements of a regime of truth. Although the selected security strategies approach the idea of truth in an indirect and rather implicit manner, they stand nevertheless into the matter through a consistent use of semantical, ideatical or contextual substitutes, and also through narratives on related problems. These official documents contain an impressive body of statements and practices that concern the dynamics by which truth related issues are addressed (understood, framed and managed) through security ideas and processes within the Romanian and German milieus.

Keywords: *(regime of) truth, security, crisis, order, rules, normalcy, Romania, Germany.*

* PhD stud. in International Criminology, Hamburg University, Germany, iulian.diculescu-blebea@studium.uni-hamburg.de

More than just formalities, Foucauldian "monuments"

In order to evaluate if and how truth is treated as a matter of security, I started by looking at a number of key documents, namely top level strategies and programs that are produced, usually, within a collective bureaucratic process and then assumed or approved at the highest political level. For a meaningful comparative approach, two very similar types of such documents, adopted in Germany and Romania, will be further analyzed. First, the national security strategies: the *2016 White Paper "On German Security Policy and the Future of the Bundeswehr"* and *The National Defence Strategy 2015-2019 "A Strong Romania within Europe and the World"*. Secondly, the cyber security strategies: the *Cyber Security for Germany 2016* and *The Romanian Cyber Security Strategy 2013*.

The documents, in their wider variety of forms – letters, transcripts, files, tickets, laws etc. – appear as ubiquitous instruments of many social organizations. This study assumes a Weberian point of view on the "modern officialdom" and the idea that its functioning is "based upon written documents ('the files')" (Weber, 1968, pp. 956-958 and 999-1001). The official documents represent a very useful starting point, as they convey the formal approaches at work in a society, the approved or authorized ways of thinking and acting, often being able to confer legitimacy or authority. Also, the fact that they are written has a special relevance in our modern culture, as the written word ambitionates or at least is expected to demonstrate a certain resilience in time, bearing a certain "symbolism of permanence" (Navaro, 2007, p. 84). As Hodder says, this kind of "mute evidence […] unlike the spoken word, endures phisycally" (Hodder, 2012, p. 171). Despite the relatively bureaucratic process, their authors most often hope to cover key issues of the matter they try to address, to make statements that would be approved or at least obeyed, that would be judged as truthful or at least appropriate. The fact that such documents mobilize both ideas and actors in a temporally remanent form, as implied since the well-known Latin adage *scripta manent*, makes them sources of first interest when it comes to researching how specific issues are understood, framed and governed.

Foucault also raised this issue of the "questioning of the document" and emphasized an essential shift in perspective from understanding documents and what they say as a basis for the reconstitution of the milieu/past from which they emanate (the memory task), to trying to "work on it from within and to develop it" and to "define within the documentary material itself unities, totalities, series, relations" (Foucault, 2002, pp. 7-12) (the archaeological task). As he wrote, „we must grasp the statement in the exact specificity of its occurrences; determine its conditions of existence, fix at least its limits, establish its correlations with other

statements that may be connected with it, and show what other forms of statement it excludes" (Foucault, 2002, p. 31). The Foucauldian approach of the documents is archeologically and it is realized by "turning documents into monuments" which means "nothing more than a rewriting… a regulated transformation of what has already been written… the systematic description of a discourse-object" (Foucault, 2002, p. 157).

Implicit but extensive approach – the truth and nothing but the whole system of it

At a first sight it would appear as quite an unexpected thing for such official documents – high level strategies and programs – to refer to the problem of truth. According to the usual common sense, truth seems to belong to another register of ideas and thinking, more philosophical and less strategic, rather ideatical than formal or bureaucratic. Nevertheless, a hermeneutical approach of the selected security strategies and governing programs, with focus on their specific perceptions and understandings, on their actual and latent content, indicates how and in what a surprisingly extensive manner these documents address issues and matters related to the core elements of a regime of truth.

By regime of truth I point, in a clear Foucauldian line, to something conceptually wider than the truth by itself, to a larger framework of many constraints within which truth is produced and that, alongside with a number of enduring common features, has also specific elements for each society and period of time. According to Foucault, this regime is a systemic arrangement that concerns: 1) the acceptable types of discourse; 2) the mechanisms and instances for separating true and false; 3) the means by which each is sanctioned; 4) the techniques and procedures valued in the acquisition of truth, and 5) the status of those establishing what count as true (Foucault and Gordon, 1980, p. 131). Looking at these elements it is easier to understand that most of the battles "for" truth, or at least "around" it, are not actually conducted "on behalf" of the truth directly, but concern rather the status and the role it plays, or the rules that separate the true and false, in a word, its regime. Most of this regime is not as much about the truth itself, as it is about nearby social acts, ideas and practices.

One of the very first things to underline is that all the cited documents address the idea of truth in an indirect and rather implicit manner. There is no explicit reference to the word "truth" as such, as a common noun, nowhere in the texts under analysis, and only in rare instances appear some direct declensions of it, mainly as adverb or adjective in rather linguistic constructions: "it is true that…" (Germany *White Paper*, 2016, p. 64), "true mutations of…" (Romania *Cyber*

Security Strategy, 2013, p. 4). Nevertheless, the documents stand into the matter through a consistent use of semantical, ideatical or contextual substitutes. And by doing so they get to deal with aspects that constitute or contribute to the systemic arrangement of the main constraints/conditions that counts for the establishment and circulation of truth within the Romanian and German political and security milieus. The truth is not approached directly, but through different substitutes or, mostly, through narratives on related problems, such as: the knowledge as the main way to track and acquire the truth about *dangers*, seen as a central security need and structured in an almost axiomatic way; the ubiquitous crisis of a deeply challenged social order that affects our lisibility, understanding and handling of key information or social realities; the grey spaces, uncharted or porous, such as the cyberspace, where true and false as well as their respective agents are hardly distinguible; the security culture as an important complement to knowledge, including a constant awareness and "appropriate" sets of ideas, practices and behaviours for the citizens; the security understood as human made normalcy, with consequences on related truth seeking, establishing and telling practices; and many others, such as the information, the data, the seal, the safe use, the certified product etc. These are treated within the next sections of this study and most are common for both Romania and Germany, except for some specific national elements.

Altogether the documents converge and create a rich official metanarrative that frame and prescribe the acceptable discourses on how the world *actually is* (crisis, unsettlement, mutations), on how it *should be* (order, stability, normalcy) and on what it *should be done* (to know, to behave, to care...) according to certain conditions and rules. There is a clear tension between description and prescription, between the actual state of German and Romanian security milieus (abnormal) and the ideal (yet "normal") , and this gives to the official meta-narrative a sense of crisis and exceptionality that empowers the actional dimension of these documents, the "should be done" part.

In addition, all these strategies and programs count among the highest level national documents and, as such, they have an impact on major social settings and practices, and also a strong constitutive effect: they establish key policy and security objectives, they offer guidelines and instructions *for* (and, of course, *about*) the security apparatus, they indicate the acceptable discourses about the security environment, they also provide the highest political narrative on security issues and this narrative also addresses matters that are relevant for the professional and social handling of truth.

Some of the values and principles whereupon the whole strategic act is claimed to be grounded, as well as the security interests and objectives are clearly related to the general idea of truth and very important for the narrow

institutional and the wider social handling of it. In the Romanian case for example, the value of "dignity" (Romania *National Defence Strategy*, 2015, p. 7) not only converges and shares a similarly positive status, but also requires the idea of truth telling as a measure of respect, which is missing in the case of its main counterparts, namely the lie, fake or false. Also, the principles of "continuity", "predictability" and "legality" clearly conflict with what a crisis represents. The national security interests derive from the constitutional provisions and are related to "*legitimately* promoting and safeguarding" (Romania *National Defence Strategy*, 2015, p. 8) a series of core values. The *legitimacy*, which implies a system where authority is both claimed and accepted as proper for the society (Lipset, 1983, p. 64), is also important for the actual operational functionality of the main constraints within which truth is established. Not least, the national security objectives include, among other, the idea of "protecting the decision-making process against influences and/or illegitimate or non-transparent actions" (Romania Defence Strategy 2015, p. 9) – which is a direct reference to the typically sanctioned acts of manipulation, deception, espionage, blackmail, corruption etc. These all represent actions that imply different misuses of both truth and lie, and that affect the authority's ability to find or establish the relevant information, the actual "truths" it needs, and to autonomously act upon that base. In essence, it ensues there are uses of truth and lie that are officially accepted as convergent with the established set of values and principles, with the security interests and objectives, and others that are not tolerated. The latter category is so important that it is treated as a high matter of security and it receives the particular status of a "national security objective".

The German security policy is also presented as "tied to values and guided by interests" (Germany White Paper 2016, p. 24). Among the four (constitutional) values that are named, two are interesting – the *human dignity* and the *rule of law* – in the sense that they tie the federal policy first to an *axiological* content which is hardly favourable nor compatible to lies, fakes, false or even to the idea of crisis, and afterword to a more neutral *normative* content where truth may well be required or sanctioned, depending on specific legal conditions. Then, one of the main security interests is to "maintain the *rules-based* international *order*" (Germany White Paper 2016, p. 25), which amounts to a view of regulated world affairs, reinforced by the mention that the named order must be maintained "on the basis of international law". Furthermore, there are measures that Germany tries to embed in larger instances – namely, EU, NATO, bilateral/regional cooperation, and international law – and according to its conception of "security in the digital age" (German Cyber Security Strategy, 2016, p. 39) aim at enforcing specific requirements such as: the use of electronic *identification*, *signature*, *seal* and other *trust services*; the problem of *allocation/*

attribution of cyber-attacks and the necessary *exchanges of information*; the spread of *trust- and security-building measures*. All these represent basic practices that are essential for a minimal infrastructure for dealing with truth related issues: to know, to certify, to establish, to trust etc. And although they may not purposefully be intended to do so, they nevertheless contribute to such a system of knowledge and power. In this particular context, it becomes obvious that the strategic effort is not exclusively focused on the truth *per se* (identities, statements, information etc.), but it supports and aims at a more general *system of it* which must respond to requirements such as clarity, order and trust.

In both counties, there are actions that are officially considered as mishandlings of the truth – as they seem to affect its social status or contradict the already established uses of it – part of them being governed as risks and threats, as key security matters. These are not only affecting certain particular truths (from a simple information to more complex decision making processes), but have a wider negative impact on social values and principles, on security interests and objectives, on social arrangements and the order within which the respective truths are established. From this perspective, mishandlings and their agents affect what truth was agreed to be in that society, his common rules, instances and means. Then, not only the truth by itself (as a basic statement or the more general idea of it) represents a matter of security, but even more so the practices that revolve around it, how it is established and used, with which purposes, how it is distinguished from false etc. The security prism, with its "myopic and colonizing properties" (Goold, Loader, and Thumala, July 2013, p. 12), is not only interested on the truth *per se*, but on the wider *system of it*. In other words, the entire regime of truth is a matter of security, including the practices that it induces and that sustain it and the changes or crises that it suffers.

Being interested in all these nearby / collateral ideas and practices, related more to the power and knowledge dimensions of truth, the official documents move away from the well-known solemn oath regarding "the truth, the whole truth and nothing but the truth", towards an approach that concern a much wider and deeper social field. I appreciate that this extended field of official interest and agency could be very well named through a paraphrase: the truth and nothing but the whole system of it.

Under the signs of crisis and exceptionality – "the world is unsettled

Foucault warns that the regime of truth "is not merely ideological or superstructual" (Foucault 1980, p. 133), but the very "condition" of the formation and development of entire systems such as the capitalism, the

socialism etc. It therefore ensues that a crisis of the regime of truth – as a whole or through any of his core elements – represents a fundamental problem at the very crux of a system or a society and induces vulnerabilities, risks and threats, namely the precise constituents of a security matter. In this context, such a crisis also implies changes in the knowledge and power settings, through emerging actors (especially those who contest the established regime, are contemptuous of it or simply careless) and a series of discourses and practices that further influences its evolution, and finally the adjustment of the former systemic arrangement or the making of a new one.

The most obviously shared idea within the official documents under analysis is that the current security environment is, as the rest of the world, at the same time more threatening and difficult to understand, less visible and accessible for the instruments that contemporary actors use in order to access or establish the truth. The overall situation is characterized under the signs of crisis and exceptionality, especially from the power and knowledge points of view: power is shifting; profound changes; intricate security situation, complex, volatile, unforeseeable; unpredictable dynamics; uncertainty of intentions; blurred borders; deficits, declines and disintegration etc. While dangers seem to multiply, common perspectives, truths, even simple facts appear harder to agree upon. All this affect our capability to know and establish the threats, risks and vulnerabilities which represent key matters of security where an accurate truth acquisition (with at least as possible of its counterparts such as lies, fakes, false, disinformation etc.) is deemed to be vital for a society. In addition, the digital transformation contributes to a large-scale crisis phenomenon that affects the society as a whole, not just the cyber space, and the multitude and dynamic of changes makes the usual quest for truth more difficult and less successful.

The Romanian National Defence Strategy 2015-2019 begins by repeatedly acknowledging the "paradigm *changes*" (Romania Defence Strategy 2015, p. 3, 5, 6) of the national defence and security concept that are related to the "increasingly *unpredictable* dynamics" of an "*intricate*" security environment (Romania Defence Strategy 2015, p. 5). The current period of time is characterized as one where multiple risks, threats and vulnerabilities "*intersect* and *overlap*", acquiring "*new* dimensions", resulting in "*unforeseeable* effects" (Romania Defence Strategy 2015, p. 5) and "strategic *surprises*" (Romania Defence Strategy 2015, p. 6) at virtually all levels, national, regional and global. Changes, surprises and complexity, as well as the inability or impossibility to know, predict and foresee are all framed as part of a relatively *new* problem that is more specific for the *current* period of time. The document depicts our contemporary period as being, at the same time,

highly threatening and difficult to understand, risky and hidden, with threats that proliferate and vital truths (i.e. about dangers) that are harder to establish. One could also say that, not knowing (in)security's truths has negative consequences – causing and amplifying or at least exposing to risks, threats and vulnerabilities – and this seems to become the matter that dominates the strategic discourse.

Among the seven *threats* to the national security, two are of interest: first, the "increasing fundamentalist *propaganda*" that favours radicalization and extremist/terrorist actions (Romania Defense Strategy 2015, p. 15); secondly, the "hostile *informational* actions" that may affect projects and decisions at the state's level (Romania Defence Strategy 2015, p. 15). Both imply practices that are considered contrary to the accepted types of discourse or that threaten the established status of those in charge with state decisions. Three other threats are voiced in terms of "instability" and "distortions" that alter Romania's security (Romania Defence Strategy 2015, p. 15), which reinforces the conservative stance and the negative strategic discourse on crisis and change. The same type of discourse is adopted for the presentation of the main *risks*, pointing towards the negative security consequences of different "instabilities", "trends" or "distortions" (Romania Defence Strategy 2015, p. 15). In addition, a number of *vulnerabilities* are held responsible for limiting the state's "ability to assess" (Romania Defence Strategy 2015, p. 16) the threats and risks. Evidently, this is not about the truth itself, but it represents a related or nearby problem because it affects the state's grip on the information that it needs about the threats and risks, and these information must reflect the truth as accurately and completely as possible. If not, the document sees a security problem, namely vulnerability.

"The world is unsettled" – the crisis-aware mood of the White Paper on German Security Policy is established from the very first words of the opening remarks by the federal chancellor, Angela Merkel (Germany White Paper 2016, p. 6). This precarious state of a "changed security situation" is something that one can "see and feel" through the impact of "crisis and conflicts" tending to replace "peace and stability" in ways that "would not have believed it possible". These are very strong affirmations, first by their appeal to the very basic senses when referring to the current crisis, secondly by openly admitting a state of strategic incredulity when considering the consequences of the crisis. The German security environment is further described as "complex, volatile and dynamic" and therefore "unpredictable" (Germany White Paper 2016, p. 28), each of these attributes portraying a problematic milieu for knowledge practices that are intimately related to the seeking of truth. In addition, the repetitive use of degree adverbs like *more* or *increasingly*, clearly frames a trend within the security

environment that, without necessarily amounting to a crisis, raises a number of challenges. The international, also decrypted as an "order in transition", is undergoing "profound changes" that are said to be driven by the increasing interconnectivity of our world. First of all, this brings "better access to information" (Germany White Paper 2016, p. 28) for more people, which potentially equals with better prospects for searching and finding the truths each one may be looking for. Secondly, it also results in "interconnection and spread of risks as well as their repercussions", among which are explicitly indicated the "information operations" – a specialized practice that revolves around information as an element of power, not aiming at truth or lie, but using them as means to power related ends. Hereabouts, the document widely opens towards the idea that specific misuses of truth, such as the information operations, are risky, repercussions and simply inacceptable for the security of a society.

The White Paper treats these changes as part of a more general crisis of the current order, under the pressure of different drivers, such as "deficits" in identity and legitimacy, "declines" in norms and values, "disintegration" of state centred orders (Germany White Paper 2016, p. 29). This image of a 3D challenged social order (deficit, decline, disintegration) does not offer a favourable background for any type of systemic arrangement, for stable and undisputed regimes. On the contrary, it may represent one of the reasons for the widely perceived crisis of many power and knowledge settings. For example the state, one of the main modern social and political constructions, that is here qualified as "the central element of order" (Germany White Paper 2016, p. 29), appear to be challenged in many parts of the world, in ways that are contributing to conflicts and crises. The strategic narrative could not have been clearer in this instance – challenges to order affect security! – and imply a logical choice in security matters: *order* is preferable to *crisis*!

In order to cope with such a milieu, the White Paper underlines the need of being "fully *aware*" of it, a prescription that blends the seeking of knowledge/truth with an ambitious monitoring discipline. It's also worth noting that this prescription adopts the imperative tone of an ultimative warning – "*only* by being *fully* aware…" (Germany White Paper 2016, p. 29) – and frames itself as a comprehensive sine qua non condition. In other words, without a fully-fledged awareness, security is not possible. Not knowing some emerging risk trend, not being aware of a remote challenge would then represent an exceptional security matter and would severely hinder the entire security policy, from its ability to "target the causes" to the capacity to "anticipate future developments". Fuelled by this accentuated awareness, the White Paper also formulates many political prescriptions that are intended to address this state of unsettlement and insecurity, the most relevant being an

absolute rejection of *crisis* ("at all times, our aim should be to prevent crises and conflicts"), a stronger devotion to *order* ("greater commitment to security, peace and a rules-based order") and a focus on *resilience* ("throughout government and society") (Germany White Paper 2016, p. 29).

In a world where "power is changing - power is shifting" (Germany White Paper 2016, p. 30), the White Paper tries to prepare the German security for a new and dangerous global order that risk to "weaken the universally binding nature of the foundations and institutions of our current global order" (Germany White Paper 2016, p. 31). The strategic stance is clearly opposed to the weakening of the core elements of the current order, which is framed as a threatening trend that must be countered. There is a concrete situation that is explicitly treated within this frame: the "rules-based Euro-Atlantic order of peace and stability" (Germany White Paper 2016, p. 31) called into question by Russia, by using hybrid approaches that "purposefully blur the borders between war and peace" and by creating "uncertainty about the nature of its intentions" (Germany White Paper 2016, p. 32). At this point, the main problems are truth related: "blurring the borders" makes truths harder to distinguish, while the "uncertainty of intentions" has a similar effect and also reduces trust. Therefore, for a solution, what appear to be important from a security standpoint is the "consistent adherence to existing and proven common rules and principles" (Germany White Paper 2016, p. 32) – in a nutshell, proven rules are essential to security.

The strategies analyzed are deeply rooted in- and animated by the idea of a profound crisis of our current knowledge capabilities, of our emprise on the truths of the security environment. The official documents suggest different crisis dimensions and their respective consequences, and each time these are framed as matters of security, mainly because they are perceived as sources of insecurity. The narrative of an "unsettled world" illustrates an synthesizes very well the crisis-aware mood of these security strategies, their inner *Zeitgeist*, and offer the image of a deeply challenged social order, affected by fundamental changes in all areas, from ethical to technological, from individuals to states, from acceptable discourses to truth handling practices. There is here something of the typical process described by the securitization literature (Buzan et al. 1998), that way of presenting a particular milieu or the entire world by pointing to vital dangers and challenges, and then to the exceptional means that need to be enacted in order to deal with them. And it worth observing that this is the case with all documents analysed, which means that the highest official discourse contributes to a general securitization process of virtually all the major "lectures" concerning the world we currently live in. This observation

confirms and complements other findings about a multiplication of the actors who feed the public fears and enable security to "trump" other considerations and values (Zedner, 2009).

Despite some minor and rather rhetorical openings towards what a crisis may imply in terms of opportunities, the strategic stance is very clear and eager to show that challenges to order affect security and that *order* is systematically preferred to *crisis*, from a security perspective. All these documents operate with an absolute rejection of crisis, which is treated as a danger (the very basic security matter), including by a plethora of prescriptions that are meant to address it like a threat. Even the security's "normalcy" and the corresponding ideal securitizing moves are framed in terms that essentially imply to prevent or overcome any kind of crisis, obviously including the one surrounding the handling of truth. One could say that, given the special place and status of the crisis as a danger construct, security documents embrace a *crisophobic ideal*, which – in a paradoxal way – transforms any crisis, actual or potential, into a matter of security, into something to secure.

Therefore, not only different particular truths and the rules that surround their social uses are treated as matters of security, but even the crises that current regimes of truth are facing. All these official documents indicate in an indirect but rich manner the increased dilution or irrelevance of traditional milestones and truth establishing practices, the shrinking of our capability to separate truth from false in key security problems, the rather *ad hoc* and exploratory search of means intended for sanctioning each other, the uncertainties around who and how could decide what counts as truth when security is at stake, the need for new techniques and procedures to be adopted for securely handling the truth etc. These problems and many other punctual issues not only contribute to the general *perception* of a crisis, but are also indicative of *how* the crisis itself becomes a matter of security: beyond the already discussed crisophobic official stance of security, we also notice a gradual overlapping of the symptoms of the crisis affecting different elements of the regime of truth over key themes of security. As a danger construct, the crisis of truth related problems is thus connected to a series of securing ideas and acts that makes it a typical security matter, as defined in my theoretical perspective.

Establishing truth within a virtual space – the cyber

Despite its virtuality, the cyber is officially understood and presented as the forestage, the *proscenium* of more fundamental social changes and

crisis, as a truly dangerous space. It is considered to be the scene of real threats that can also have an impact in other physical or social spaces, and its characteristics raise challenges to some of the most usual truth establishing practices of a state. This particular status comes especially from the fact that, in the cyber space, it appears to be even more difficult to establish or sanction truth and its counterparts, which represents a major social preoccupation and, as we have already seen, also a matter of security.

The Romanian Cyber Security Strategy 2013 underlies the major impact that the modern technologies had on the entire society, resulting in "true mutations" within its inner "functioning philosophy" (Romania Cyber Strategy 2013, p. 4) in all major social areas, as well as in the daily life of the individuals. The use of the term mutation here is very interesting, especially as its primary use in biology refers to permanent changes in the sequence of an organism's DNA. In this context, the reference to "true" seems to play more as an emphasis for the fundamental character of the changes that the society is undergoing, a paraphrase for crisis within the very core of the modern social, a crisis through which the technology becomes a central premise or an even ontological part of what contemporary society is, of its social DNA.

The cyber space is defined as a "virtual" milieu (Romania Cyber Strategy 2013, p. 7) – therefore not exactly real, but rather a computer generated or simulated one – that includes both the informational content and the users' actions. Despite the *virtual* nature, the cyber, just as other security environments, is framed as a *dangerous* space, with consequences that trespass its bodiless borders into the *real* physical or social spaces. Many countries have experienced cyber-attacks and even preparing for "conflict in the virtual dimension" (Reveron, 2012, p. 4). Therefore, (in)security is understood as an ubiquitous issue, beyond virtual or real spaces. Within the cyber-space it is very difficult to establish or sanction truth and its counterparts, which causes a plethora of anxieties. Moreover, its gradual expansion would "introduce vulnerabilities" (Romania Cyber Strategy 2013, p. 4) in the society and it is then framed as a special issue that "must" be treated as a "major preoccupation" by all actors involved – a typical securitization approach. The combined deduction of the two ideas is that a milieu where minimal truth requirements (identities, statuses etc.) cannot be established represents a security problem, both as source of dangers (risks and vulnerabilities) and as a challenge for the acting system of power.

This new and threatening cyber appear as a space that must be secured and the strategy aims at a "*safe* virtual milieu" that should be highly "resilient and trustful" (Romania Cyber Strategy 2013, p. 6). Beyond the fact that the concept of resilience has been imported in many security and

governance challenges (Aradau, 2014, pp. 73-87), it is interesting to observe how security is based on characteristics that are also important for the functioning of a regime of truth, namely its ability to withstand punctual attacks / contestations or a more general crisis (resilience), as well as an underlying confidence or acceptance of its main actors, speeches and practices (trust). Security and regime of truth appear to share a number of common conditions.

In a similar vein, the Cyber Security Strategy for Germany 2016 underlines right from the introduction the accelerated and profound social changes that are brought by digital transformation, which "radically changed Germany in just a few years" (Germany Cyber Security 2016, p. 4). *Change* is the key-word and it describes processes that characterize not only the cyber space, but the society as a whole, indicating a large-scale crisis phenomenon, in its general and etymological Greek sense of a time with risks and opportunities, when important decisions must be made. In this context, it is the state who "has the duty to assess and act" upon these processes of change, as the most prominent actor, alongside with industry and other stakeholders. Because of the acute perception of a crisis situation and of the risks it implies, two correlated issues are raised, first the need for "trust" and "confidence", and secondly the status of security as "an essential aspect" (Germany Cyber Security 2016, p. 4). This implies that overcoming the crisis would not be possible without a viable nexus of *trust* and *security*, both being mainly in the responsibility of the State.

Further concerns are related to the diversity and status of the attackers (states, groups or individuals, often with "criminal, extremist/terrorist, military or intelligence background") and the methods for concealing that "complicate detection, mapping, defence and prosecution". It is, basically, the problem of perpetrators hiding the truth and defenders not knowing and/or being able to establish the truth about who-did-what and whom-to-punish – which raises an "especially large risk of uncontrolled escalation", a serious security matter. This challenges to the usual truth establishing ambitions of a state, namely the classical police questions of *who* to identify as perpetrators*, what* they do, and *how* to deal with them – and answering these questions is essential for the functioning of a security apparatus.

At the end it becomes obvious that – from an official perspective – the virtual cyber-space is not only the *forestage*, the *proscenium* of changes that technology brings into the modern societies and which allows the state (and also other social actors) to make predictions and plans, to access or even produce future truths ahead of time. The cyber is also the *entire arena* where spectators and actors, citizens and/or users can see (and interact with) a state trying to

replay the historical piece of establishing typical governmentality mechanisms over a new space and its social relations. The cyber in its entirety, including rules for handling the truth, appear as a socially and technologically emerging construct.

An official and axiomatic system for the knowledge-security nexus

The problem of the correlation between *knowledge* and *security* is a matter that dominates the strategic discourse and is visible in each of the official documents under analysis. While references to *knowledge* may appear as a partial link to the truth itself, in fact they include most of the wider truth related issues that are of interest from a security standpoint, namely its acquisition, its separation from false, a set of particular skills in approaching and dealing with truth and its counterparts. Taken together and synthesized, these various references form an almost axiomatic system of ideas and statements that are treated as self-evident or necessary truths. The first axiomatic idea that knowing the (truth about) dangers improves the security odds as it offers the basic conditions for some of its very important practices and / or statuses such as anticipation, prevention, signalization, predictability, and understanding. *Reciprocally*, not being able to establish the truth about dangers means less security as it amplifies vulnerability or, with the exact words employed by the documents, it translates in unpredictable dynamics, unforeseeable effects, strategic surprises, or lack of understanding. *Complementarily*, the distortions and counterparts of truth generate insecurity in multiple forms: instability; hostile propaganda and informational actions; vulnerable decision-making process; influences and/or illegitimate or non-transparent actions etc.

Against the fallible epistemological background of an unpredictable and difficult to understand security milieu, in order to manage a large array of issues considered to be "vital", the Romanian National Defence Strategy points towards the need for "*knowledge* of evolutions in the security environment" (Romania Defence Strategy 2015, p. 6) which is treated as being "of paramount importance" (Romania Defence Strategy 2015, p. 11). Knowledge is here understood as a *recognition* of something that exists and manifests in the world, as a *narrative* or a *tale* of the world that "tracks the truth" (Nozick's influential "tracking theory" of knowledge) (Nozick, 1981, pp. 167-196) and that should not be affected by the counterparts of truth, being "neither fictions nor opposed to facts", although "always inmmersed in history and never innocent" (Escobar, 1995, p. 19-20). Such a narrative is bound 1) to correspond to evolutions in the environment (i.e. a correspondence approach

of truth) and also 2) to be of interest from a security perspective (i.e. to concern risks, threats or vulnerabilities). These two validity conditions, of truth and relevance, describe very well a kind of "situated knowledge" (Haraway, 1988, pp. 575–599), one that is specific and corresponds to certain situations. The security strategies do not aim at a purely scientific knowledge even if research may punctually be involved, but at this type of situational knowledge that is expected to be both true and actionable, which indicate a rather pragmatic approach. At what Foucault calls a "preconceptual level" (Foucault 2002, p. 68), security documents cannot make an appropriate use of the idea of knowledge, more precisely of the "need for knowledge" without first implying a relation of dependence of knowledge to truth. In the absence of truth, knowledge cannot define a domain of validity for itself within the security field, as maybe in any other field. This is why, without bothering with too complex epistemic or philosophical considerations about the relation between knowledge and truth, the official documents embrace the naïve realism of a knowledge that simply has to track/represent the truth about security matters of interests, to be able to separate it from fake, false or misleading. They signal that truth is an essential condition of the knowledge they praise, which is not explicitly stated, but also not less important for that reason. Truth is not confounded with knowledge. Nevertheless it represents, in this context, its most basic requirement, a constitutive criteria in the absence of which one could not speak of *knowledge* or at least that would not respond to the *need* praised by security documents.

This need for knowledge also induces the reciprocal idea, namely that not knowing certain evolutions in the environment hampers the ability to "responsibly manage" their impact, thus affecting the security of the country. The strategic prescriptions given by the lines of action add a new emphasis on "*knowing* the risks and threats *in all aspects*" (Romania Defence Strategy 2015, p. 18), on "*understanding* the nature of threats" through scientific research (Romania Defence Strategy 2015, p. 21). Moreover, the lines of action established for the intelligence, counterintelligence and security dimension are of special interest through their bold emphasis on one hand on "*knowing*" and "*identifying*" different threats, and on the other hand on "*signalling*" and "*drawing attention*" to the established beneficiaries (Romania Defence Strategy 2015, p. 19-20). In essence, this describes the functions and priorities of a systemic arrangement for seeking, establishing and circulating the knowledge regarding security matters, while also bespeaking its fundamental character.

Moreover, the broadening of the "*anticipation* capacity" is considered nothing less than "fundamental" and the development of systems for the

"early spotting of dangers" is qualified as "mandatory" (Romania Defence Strategy 2015, p. 18). Again, the main idea is that (early) knowledge and the related capacity to establish truth preserves a larger room for action on social situations that have not (yet) developed into real crises or conflicts. A strong assumption is made, namely that a well informed and opportune action on a truly dangerous situation will prevent it to become true. It is a positively valued so called "self-denying prophecy", a special kind of knowledge that – when coupled with the right action – would falsify itself by changing the social realities. This assumption emerges quite often within the security professional culture and it is quite relevant for the regime of truth because it means that it is good to bend the-now-true-course towards a threatening reality, by acting on key conditions in order to falsify that course and prevent him to become true. It means that – for security purposes, for order or stability – one can and should falsify a (potential) truth and replace it with another, more suitable, social reality.

In order to resume, knowledge and the related capacity to establish truth about threats and their perpetrators offer more options, time and space for security oriented action. Not knowing (in)security's truths has negative consequences, causing, amplifying or at least exposing to risks, threats and vulnerabilities. It worth noting the dramatically staging and justification of the need for knowledge (paramount, vital, mandatory, fundamental, in all aspects etc.), which are further enhanced by a very contrasting accent on the current problems and limitations (unknowns, intricacies, complexity, unpredictability, uncertainty etc.). The actual content and also the tone of these texts express a sense of inadequacy between means and challenges, a state of crisis for our knowledge capabilities that would not be up to security needs and requirements, and thus would not allow for an adequate "tracking" of truths related to key matters of security. When the latter happens, resilience understood as preparedness for crisis and being able to cope (Omand, 2010, p. 57 and 63) appears to be the last resort/hope for the strategic narrative: who is unable to know or to establish the truth should, at least, be able to resist and to manage the consequences. For the strategies and programs analyzed, these principles appear to have enough consistency and coherence, practical relevance and general applicability, and they are so thoroughly used that they became an official and axiomatic system of thought about the knowledge-security nexus.

Specific elements of national narratives

The research question has also a comparative dimension, with focus on the meta-narratives that are produced in relation to the core elements of

the regime of truth in the respective German and Romanian security contexts. Tellingly, while most of these are commonly shared by the two societies, there are also aspects that are specific to their respective German or Romanian security context, and that are not consistently reflected within the documents of the other country. These differentiations seem to be rather local nuances and do not indicate a strong contrast in the approach of truth, but are nevertheless important for the comparative perspective of this research.

The Romanian specificity is given by the worries and prescriptions surrounding a two folded idea, focused on unity and status. Firstly, they regard the inner *unity* that must be achieved through "national *cohesion* and *consensus*" (Romania Defence Strategy 2015, p. 6). Moreover, one of the main principles for this process is the coordination through unitary conception and plans. The strategy formulates hitherto a statement that not only matches the classical coherence approach of truth, but (more important for the theoretical perspective of this research) also sets the *national* arena as the main framework in which the Romanian security apparatus deals with the truths that it seeks/produces/ manages, and gives a certain political dimension to the process. Secondly, there is a solid concern for the symbolic *status* within the world, which results quite clearly from the will to strengthen the "strategic *credibility*" based on "*continuity* and *predictability*" (Romania Defence Strategy 2015, p. 6) as well as from the cautious legitimating of the nature and performativity of the national security interests (Romania Defence Strategy 2015, p. 8).

The German particular approach is based on two elements, namely rules and a strong emphasis on collaborative approaches. Firstly, out of security interest, Germany is on the pursuit of a specific type of order (Germany White Paper 2016, p. 52), an order that is based on *rules* (norms, values) rather than on other regulatory elements such as the known Smithian invisible hand, historicist determinism, religious visions etc., and that is clearly pro-regime and anti-crisis. It explicitly states "right, not might!"(Germany White Paper 2016, p. 53). Secondly, security related truths are better found/established within structured arrangements, in *cooperation* with other relevant actors and according to specific rules and procedures, in "integrated networks of actors and instruments" (Germany White Paper 2016, p. 15), among "reliable and dependable partners" (Germany White Paper 2016, p. 8) that "embrace mutual interdependence" (Germany White Paper 2016, p. 23) and combine their expertise to "create a clear overall picture" (Germany White Paper 2016, p. 50) – a systemic arrangement that even implies a "cross-generational responsibility" and, obviously, tends to embrace the coherence declination of truth. This also gives a certain political dimension to the process and establishes the *European and international* arena as the main

framework wherein the German security apparatus deals with the truths that it seeks, produces or manages – but still observing "a clear national position" (Germany White Paper 2016, p. 25). Overall, a key supposition became obvious, even if not directly stated, namely that shared security implies a minimal common framework of truth and trust, as a necessary condition and basic infrastructure for enhanced security cooperation. The same approach is adopted for the governing of the cyber space, through measures that facilitate cooperation, exchanges and inclusion: government and business must "work closely together" at all levels and have a "trustful" and "intensive" exchange of information, surpass the IT skills shortage through "networks of specialists" and "personnel exchange programs" (Germany Cyber Security 2016, p. 21). For the German strategists, security is a "whole of society endeavour" (Germany White Paper 2016, p. 58), just as a (the?) grand and coherent social truth.

An official Faustian pact – truth as a mean towards security

The official security discourse of these documents addresses a long list of problems – old phenomenon and new changes, known and even unknown threats – and for some of them it requires extraordinary measures beyond politics as usual. The way in which the official documents approach truth related issues and critical situations that affect its "normal" uses is indicative of a perceived crisis of the regime of truth. And this is a problem that concerns my research: why and how unfolds this framing of truth and its counterparts in relation with dangers – risks, threats and vulnerabilities – rather than with ideas such as opportunity, positive social changes or some new philosophical basis for the understanding of truth. According to the narratives analyzed, the securitization of truth, of its regime and crisis, does not appear as the exclusive result of new and successful speech acts coming from official actors within the society. It seems that it is based rather on an already solid understanding of the status of truth as a mean (among other) towards security as end. The texts made it clear that security has a higher strategic and official status and, as such, one can or even should transact truth in order to achieve and preserve security, especially in an increasingly dangerous environment.

This is the very motif of an official Faustian pact through which authorities set the conditions for a bargain whereby public and private actors should sacrifice something of spiritual or moral importance (*truth* in this case, but also *liberty* and other in different instances) in order to obtain social or individual benefits (*security*). These conditions are not structured as a proposal about which the different actors involved could autonomously decide, but rather as imperative lines of behaviour where the main truth

handling practices are already established, officially leaving small merges for option. The key (im)balance of truth and security is nowhere in these documents allowed to come into question, and this is how the regime of truth endeavours to prevent even the eventuality of a questioning of the structural options that subordinate the handling of truth related practices (access, dissemination, classification, en-/decryption, warning etc.) to aims of security. In this perspective, truth appears as a central social and cultural value that finds its official limits not in other supposedly immuable values, but rather in security motivated concerns and objectives, in a specific conception of security as "normalcy", in the official will and emprise over *what* and *how* gets to be established as relevant or true, or in that axiomatic understanding of the knowledge-security nexus.

Nevertheless, it is difficult to identify what exactly is truth for the official strategists. There is no direct and explicit statement within these documents and one plausible cause could simply be the fact that there is no interest for the inner nature of truth, but rather for the nearby practices that concern its establishment and acceptable uses, for its regime. While the word "truth" does not appear as such in any of the studied documents, there are strategic statements that concern how truths should be treated as means of security, which are the good and acceptable ways to handle them or, the opposite, the bad and dangerous ones. Moreover, the official security strategies do not share a unanimously positive perception of truth. On the contrary, truth is far from being treated as an immuable value, subtle but numerous distinctions being made among different categories such as useful or irrelevant truths, to classify or to disseminate, to elicit or to protect etc. The official status of truth is measured by how it fits with the needs, ideas and rules of the respective society, mainly of the state, and priority is given to those that are considered to represent matters of security. This is one of the main avenues by which security matters (as exceptional political problems), practices and ways of thought contribute to the construction / establishment of a regime of truth.

If I should still try to answer the question of "what is truth?" from the strategic official perspective, I would mostly have to point that, essentially, truth is what security – discretely – makes of it, without any further complex definition. For the strategic official approach this seems to be enough and it unveils a certain will of power/security over truth that is obvious each time truth becomes, through its regime, a mean towards another end, usually expressed in terms of security.

This way of approaching the matter speaks also about the barely visible disciplinary technologies of power and punishing mechanisms that are

supposedly directed towards some marginal "others", those who mishandle the truth, and not against the "responsible" citizens and society who observe and act and behave according to the established rules. These documents reflect and contribute to technologies of power that are centred on a *state* that is still seen as an anchor for the social order, on the generally good but endangered *citizen*, and also on the figure of a so-constructed *mishandler* of truth, a human or social actor that breach the established procedures and periclitate the "normal" order. Such a discrete but consistent securitization of the regime of truth unveils itself as an instrument of disciplinary power that is employed as a governmentality tool by the officials, politicians and security professionals. It is worth noting that within this official perspective of security understood as normalcy, to securitize a regime of truth implies the claim to normalize its state against different challenges and abnormalities that may affect his core elements or to overcome the crisis that hampers its normal functioning; in short to claim exceptional means in order to impose the norm(al) and to discourage or punish deviations.

My initial approach of such documents as objects of study did embrace a played naïveté, one that was meant to allow now to ask in a typical Foucauldian way: why the presence of such a key issue as the problem of truth within modern security documents has not been observed earlier? These strategies cannot offer a complete answer to such a question. Nevertheless, they clearly indicate that within the security milieu one can find a very consistent *interest*, a complex *understanding*, and a multitude of concrete *practices* that focus on the social uses and creation of truth. And yet, those who produced the documents did not explicitly refer to truth as a concept or as a general idea, and only implicitly addressed the main elements of its regime. Although the word "truth" is nowhere mentioned in these texts, the authors repeatedly and consistently focused rather on issues and series such as: knowledge, understanding and their limits; different distortions, manipulations, influence and propaganda practices; espionage, covert operations, subversion and other informational actions; concealment, anonymity, classification, encryption; blurred boundaries, obscured roles, hybrid threats, undetected attacks, strategic surprises; awareness, monitorization, dissemination, early warning; order, rules, normalcy; crisis, disintegration, carelessness etc. All of these belong to a wider framing of truth and they represent small units that, through series and relations, reconstitute a barely visible puzzle.

In this context, in order to try an answer to the upper question, I emphasize that this puzzled problematization of small and disparate elements, the focus on details and the use of argotic terms contribute to obscuring a deep and wide approach of the problem of truth as a matter of security – even for

those who are close or activate in the field. Furthermore, the strong perception of security as the *central* or *end* subject of these situations and actions does not help to see in the different truth related elements something more or au delá of the usual and already familiar "security issues". This security prism or perspective is increasingly popular and used not only by security professional actors, such as the police, the military or the intelligence institutions, but also by politicians, business and corporations, mass media and the general public opinion. As Buzan, Waever and Wilde (1998) have indicated with their widening of the security agenda, we tend to speak security in many sectors of the social life, from military to political, societal, economic and environmental – and by specific processes of securitization the issues are reframed, which produces new understandings and problematizations, sometimes focused more on security aims, procedures and acts, than on the initial/basic issue. This means that when a referent object such as an element of a regime of truth is securitized, one still sees the security stakes and processes, rather than their truth related object.

What still remains to be understood is whether this deeply fragmented and nontransparent framing of truth within the security official discourse is the purposeful result of a conscious conduct, or something that simply emerges from the current professional routines and frames of thought. Regardless of the answer, with or without intentionality, their micro frames and handlings of different truth related elements contribute to the wider social and political regime of truth, having a certain constitutive effect. And this is precisely what Foucault was referring to when he indicated that documents also produce the very actors that use them (Foucault, 1991, pp. 87-104).

These official documents contain an impressive body of statements and practices that concern the dynamics by which truth related issues are addressed (understood, framed and managed) through security ideas and processes – namely the exact research problem I raised. They indicate the acceptable security discourses, what should be considered truth and what cannot, but also how the truths are to be handled by different subjects through specific practices, sometimes stating the respective consequences in case of misconduct. The strategies even establish and define specific spaces/milieus such as the cyber, the privacy, the national, the international, wherein such statements and practices can be enforced, promoted or newly created – thus playing a double role, discursive and actional, at the same time.

To resume, the official security strategies see, understand and address the issue of truth in an indirect manner, with a tendency to impose an etatist frame of mind, justifying the state's views as the acceptable narratives, mainly for reasons related to security and authority. This contributes to giving the

authority of "truth" to an official speak that, through specific practices and frames of thought, creates the truth as a matter of security and claims the authority to regulate its regime.

References:

1. Aradau, Claudia, (2014), "The promise of security: resilience, surprise and epistemic politics" in *Resilience*.
2. Buzan, Barry, Waever, Ole, Wilde, Jaap de, (1998), *Security: A New Framework for Analysis Boulder*, Colo.: Lynne Rienner Pub.
3. *Cyber Security Strategy for Germany*. Berlin: Federal Government, 2016.
4. Escobar, Arturo, (1995), *Encountering Development: The Making and Unmaking of the Third World*, Princeton: Princeton University Press.
5. Foucault, Michel, (1991), "Governmentality" in *The Foucault Effect: Studies in Governmentality*, London: Harvester Wheatsheaf.
6. Foucault, Michel, (2002), *Archaeology of Knowledge*, London: Routledge.
7. Foucault, Michel, Gordon, Colin, (1980), *Power/knowledge: selected interviews and other writings, 1972-1977*, New York: Pantheon Books.
8. Goold, Benjamin, Loader, Ian, Thumala, Angelica, (July, 2013), "The Banality of Security. The Curious Case of Surveillance Cameras" in *British Journal of Criminology*.
9. Haraway, Donna, (1988), "Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective" in *Feminist Studies* Vol. 14, No. 3, pp. 575–599.
10. Hodder, Ian, (2012), "The Interpretation of Documents and Material Culture" in *Sage Biographical Research*. Ed. John Goodwin, Thousand Oaks, CA: SAGE Publications, Inc.
11. Lipset, Seymour Martin, (1983), *Political Man: The Social Bases of Politics* (London: Heinemann), 2nd ed.
12. Navaro, Yael, (2007), "Make-believe papers, legal forms and the counterfeit: Affective interactions between documents and people in Britain and Cyprus" in *Anthropological Theory* 7: 79.
13. Nozick, Robert, (1981), *Philosophical Explanations*, Cambridge, MA The Belknap Press of Harvard University Press.
14. Omand, David, (2010), *Securing the State*, London, Hurst&Company, 2010.
15. Reveron, Derek S., (2012), *Cyberspace and National Security: Threats, Opportunities, and Power in a virtual world*, Georgetown University Press Reveron 2012.
16. *The Romanian Cyber Security Strategy 2013*. Bucharest: Government.
17. *The National Defense Strategy 2015-2019*. *"A Strong Romania within Europe and the World*. Bucharest: Presidential Administration, 2015.

18. Weber, Max, (1968), *Economy and Society: An Outline of Interpretive Sociology* (New York: Bedminster Press), 1968.
19. Zedner, Lucia, 2009, *Security*, Routledge.
20. *White Paper "On German Security Policy and the Future of the Bundeswehr"*, Berlin: Federal Government, 2016.

SECURITY PARADIGMS IN THE 21ST CENTURY

ISLAMISTIC EXTREMISM AND TERRORISM IN THE WESTERN BALKANS

Dragan Simeunović*

Abstract

The paper analyzes, by using content analysis and historical-comparative methods, the causes of the emergence and development of Islamistic extremism and compares the state of affairs regarding the presence and the tendency of further growth of Islamistic extremism in Albania, Bosnia and Herzegovina, Montenegro, Kosovo, Macedonia and Serbia. This means practically identifying the inspirers and those who spread extreme Islamistic ideas, their activities, international sponsors and contacts, their active contribution to global jihad, as well as assessing the abilities of above-mentioned Western Balkan societies to defend themselves against this growing danger threatening not only the lives and the property of their citizens, but also their democratic constitutional order. The research has revealed a significant strengthening of the number of Wahhabi believers, the increase of their aggressiveness, the violent takeover of the existing and the building of a large number of new mosques, which are out of control of official Islamic communities in these societies, also the construction of dozens of Wahhabi settlements, where sharia law is applied, not the laws of the home state. The return of their financiers contributed to the intensification of religious propaganda and to the increasing of affection for Wahhabi ideas among the local Muslim population, which resulted in the departure around a thousand fighters from the Balkans to join the terrorist organizations in the Middle East battlefields. Confronting the rising Islamistic extremism in the Western Balkans is blocked by: lack of real and quality prevention, inexperience and poor results in the deradicalization of extremists, and in some areas, the lack of political will. All of the above, mentioned together implies not only intensive cooperation between the police and other security structures of the West Balkan and the surroundings countries, but also the urgent help of adequate institutions of the International community.

Keywords: *Islamistic extremism; Western Balkans; terrorism; Wahhabism; ISIL.*

* Prof. Dragan Simeunovic, PhD, a full time professor at the Faculty of Political Science at the University of Belgrade and director of the National Security Academy, Serbia, Email: dragan.simeun@gmail.com.

Introduction

We live in a time when Islamistic[1] extremism and terrorism are very widespread as political and criminal manifestations of the adoption of jihadist ideology (Simeunović, 2016 a). Apart from the continuing conflicts in the Middle East, this is helped by globalization which allows for an increased mobility, from the level of individual to the level of migrant, by large possibilities of Internet abuse for extremist propaganda and mobilization purposes, and by the lack of definition of the extremism and terrorism at the UN level, which would make efforts made by the international community in the field of combating security challenges far more effective.

The literature on the Islamistic terrorism has become very numerous after September 11, 2001. However, literature on the Islamistic extremism in the Balkans did not follow the same trend, and has begun to appear more massively over the last ten years (Archick, Rollins and Woehrel, 2005) due to the relevance of the topic, not only for the security of the region and its surroundings, but also for the countries of the EU and the US. Also, in the literature on the Islamistic extremism in general, it is increasingly noted that a special attention must be paid to the Western Balkans as the part of Europe whose population is multi-religious and multinational (Radeljić, 2010; Vidino, 2006). However, it can be observed that the authors from the Balkans are rather subjective in the treatment of this topic, which is somehow expected in the environments that are burdened with relatively recent war events (Babanovski, 2002).

The main deficiency of this literature is that, it is often not empirically grounded. A significant corrective to this are expert reports and case studies (Azinović and Jusić, 2016, Selimi and Stojkovski, 2016) written for the needs of international institutions and organizations. Most of the literature on the Islamistic extremism in the Balkans devotes considerable attention to its history, with some disagreements, especially over the timeline when the Islamistic extremism arrived to the Western Balkans and the significance of the cooperation of Balkan extreme Islamists with the Nazis during the Second World War (Kastrati, 2015; Shay, 2008).

Also, the actors of Islamistic extremism, the content of their activities and the degree of threat they represent to the surrounding and other

[1] The expression Islamistic extremism, "with the suffix -istic, is more political correct than the expression Islamic extremism. It indicates a following, imitative behaviour, and also the potential ideologization and political interpretation of Islam, which reduces the possibility of violating the believers' feelings". See more about on Simeunović, D. (2009). Terorizam. Beograd: Pravni fakultet Univerziteta u Beogradu, p. 197.

European countries (Bardos, 2005; Deliso, 2007) are defined differently. Studies on Islam in the Balkans which try to explain modern Islam and its extreme interpretations objectively, (Bećirević, 2016; Jerotić, 2016) are quite rare. The literature dealing with the future of jihad and, in general, Islamistic extremism presents gloomy forecasts for the Balkans (Fares, 2008). There are very few scientific studies on the latest rise in Islamic extremism in the Western Balkans, generated by the wars in Syria and Iraq, as the reason for Balkan extremists to go to these battlefields. This is compensated by territorial reports (Panovski, 2011; Selimi and Stojkovski, 2016), or partial problem reports (Đurđević, Stevanović, Mitič and Kocić, 2016), which, taken separately, do not provide an accurate insight into the whole situation.

For all these reasons, the existing literature on the Islamistic extremism in the Western Balkans is treated, in this paper, according to criteria of scientific rigor. Since this paper is an attempt to determine, not so much the causes of the presence and lasting of Islamistic extremism in the Western Balkans, but its current state and the reasons for its growth over the last ten years. With this in mind, as the most appropriate method, according to the purpose and the nature of the available sources (Lobnikar, Prprović, German, Banutai, Prislan and Cajner Mraović, 2016) comparative analysis is chosen and used to determine the inspirers, perpetrators and other actors of Islamistic extremism in the Western Balkans, sources of its financing, the degree of threat to their own and to other communities, its contribution to global jihad, the relation of extreme religious groups with the official Islamic communities of the Balkan countries, as well as the ability of those countries to resist extremism and eliminate it from their communities.

While qualitative and quantitative analysis of data collected from scientific books, articles in scientific journals and collections, primary and secondary available sources, like reports and other documents from the international and state institutions, respectable newspapers and other various sources, deepens the knowledge of the general view and the main characteristics of Islamic extremism in the Balkans, which creates an objective and true picture of the topic of this work, the historical-comparative method shows us the similarities and differences between the degree of spread and the tempo of Islamistic extremism spread in various Western Balkan countries and gives a more accurate assessment of its development in particular communities. The historical-comparative method was also used to compare the situation in different countries in order to determine the specificities in each of these countries. By comparing differences and similarities it was possible to determine whether Islamistic extremism is a phenomenon of the same nature or it has a very specific form in each of these countries individually.

The aim of this paper is to give an insight into the current situation of the presence of Islamistic extremism in the indicated Balkan countries in order to make the institutional response to this situation more adequate. Determining the real situation of the spread of Islamistic terrorism in this part of Europe should make it easier to understand it, and thus take more adequate measures to fight this security challenge. The results obtained should help to create better-quality practical solutions which have their application in the fight against Islamistic extremism in the present and the future. The reason for that is not just the number of local Islamic believers, but also the presence of newcomers from the so-called "critical" Muslim countries who have brought and spread the Wahhabi interpretation of Islam, and also the large number of Balkan inhabitants who have become members of terrorist organizations over the last decade, which altogether means a potentially large number of returnees from the Middle Eastern battlefields whose potential for intolerance and conflict is extremely high.

The text is systematized in the way that the introduction gives a critical approach to the literature on the subject, gives methods and goals of work, followed by the history of the phenomenon investigated, a part about the types and activities of the actors of extremism, and then a part about the goals of extreme Islamic groups and organizations in the Western Balkan. This is followed by a section on the capability of Western Balkan societies and states to suppress Islamistic extremism as a security challenge. The paper ends with concluding observations on the results of comparative analytical research and recommendations for activities in the field of combating Islamic extremism in the Western Balkans, and a list of references.

History

Despite the popular opinion which is also shared by the literature on the terrorism, that Islamistic extremism began in the Balkans in the `90s of the 20th century, during the war in Bosnia and Herzegovina, it has a pre-history in the Western Balkans. After the sporadic appearance in the history of the wars conducted in the Balkans, the seed of militant Islam in the region was formally sown during the Kingdom of Yugoslavia, in 1939 by establishing the Young Muslims, an organization modelled and named after the youth organization Muslim Brotherhood from Egypt (Stojančević, 2016). In World War II, its members and followers cooperated with the Nazis as members of the Handžar and Skenderberg divisions (Shay, 2008).

During the period of the SFR Yugoslavia, various extremist organizations of Muslim emigrants were active abroad, usually in cooperation

with Ustasha emigration. Also, it is commonly believed that the historic opportunity for the breakthrough into the Western Balkans Islamistic extremism had during the 90`s, when numerous Islamistic militants gathered in Bosnia and became "holy warriors" - mujahedeens. However, according to some authors (Kastrati, 2015), Islamistic extremism first arrived in the late 80's in Albania along with the first pro-Iranian fundamentalist ideas from the Middle East (Bardos, 2005; Mahnaimi, 1998), and later, after that in Bosnia and Herzegovina.

Their first propagators were Islamic humanitarian organizations. The result was a parallel course of Albania to liberalization and to the "brotherhood of Islamic countries". During the `90s, Osama bin Laden organized camps in northern Albania (Kelley, 2001), while for a number of KLA members an Islamistic course was organized in Afghanistan (Hedges, 1999; Ash, 2001). Osama bin Laden was inclined to islamize the KLA, hoping that it would turn the Balkan region "into his main base for Islamistic armed activities in Europe" (Sunday Times, 1998). In 2000, a high-ranking Interpol officer informed the US Congress about the connections of al-Qaida, the Albanian state structures and the KLA, (Mutschke, 2000). Also, Kosovo's leader Ibrahim Rugova (Tanjug, 2001) pointed to KLA's increasingly pro-Islamic orientation.

Until 1992, training camps for mujahedeens in Bosnia and Herzegovina had already been established, and funded by Islamic humanitarian organizations together with Al Qaeda. Bin Laden's presence in Albania in 1994, was confirmed from several sources (Mahnaimi, 1998), as well as financing of KLA by Al Qaeda (Raimondo, 2001). Only "between 1993 and 1995 over $ 900 million had been illegally invested in extremist activities in the Balkans" (Sandić, 2011; Simeunović and Dolnik, 2013). Most of these organizations were later closed under the pressure of the United States, thus the flows of financing Islamistic extremism in the Western Balkans were cut, but only for a short time.

Certain number of mujahideen moved to Kosovo in 1998, where they formed the mujahedeen unit called "Abu Bakir Sidik" to participate in the battles. At the time of the intensification of the Kosovo conflict, foreign mujahideen from Islamic and Western states began to arrive in Albania again. This was a long process, and that explains the fact that later, they came, in a far greater number, to Macedonia where they were the main propagators of Islamistic extremism and participants in armed conflicts. The number of mujahedin and members of Al Qaeda who fought in the Macedonian ONA was around 600 fighters (Babanovski, 2002).

The further development of Islamistic extremism in the Western Balkans was in correlation with the stance of the US and other Western countries towards terrorism. When the Western policy after September 11, 2001 towards the mujahedin began to change, the policy of the Balkan states, like Bosnia and Herzegovina, became less friendly towards them, but with restraint, since a large number of mujahedeen had Bosnia and Herzegovina citizenship (B92, 2007).

The fact that about 750 people in Bosnia and Herzegovina are still under constant surveillance of western intelligence services (The Daily Telegraph, 2004), and that about a thousand extremists from the Western Balkans (of which about 65% are Albanians) went to join ISIL and Al Nusra, tells enough about a potentially high risk of the Islamistic extremism of people from the Balkans, which is mostly manifested in their massive terrorist actions in the Middle East, and occasional terrorist actions in the Balkans and in the US and EU countries.

Actors of extremism: types

Inspirers and propagandists: The vast majority of Islamic believers in the Balkans practice moderate, "national" Islam that has been brought to the Balkans by Turkey, country which still has a great influence on them, so the Balkan Muslims are not only different from the Wahhabis, but at first, they were repelled by Wahhabis aggressiveness.

Nevertheless, many sources, documents, and the testimonies of repentant terrorists (Hamad, 2007) show that the intense presence of, not only various religious and humanitarian Islamic foundations, but also foreign mujahedeen and al-Qaeda members, even Osama bin Laden himself, starting from the late eighties in Albania, in Bosnia and Herzegovina during the 90`s war, and afterwards in Sandzak, Macedonia, and Kosovo, produced significant propaganda influence on introducing and accepting Wahhabism and, according to some authors (Woehrel, 2005), this propaganda created many supporters of Islamist extremism ready to commit acts of terrorism.

That is the only explanation for the fact that, for example, in Albania, which was “the first atheist state in the world” (Prifti, 1978, p. 100), as early as the first years after the fall of the communist regime in 1990, religiousness was quickly restored primarily among Muslims who now account for 56.7% of all population, plus the number of Sufis who, according to various sources, make around 2.1%.

Several political and economic disturbances that happened, not only in Albania, but in every Western Balkan country, from the beginning of the

process of democratization, facilitated the breakthrough of the Islamistic extremists.

The current state of presence of Islamistic extremism in the Western Balkans is characterized by new trends. The main inspirers and propagandists of jihadist ideology are no longer mujahedins, but people from Balkans, mostly Bosniaks and Albanians, former students at the universities in the Arab states of the Persian Gulf, countries which had supported Bosniaks and Albanians in their fights.

These states had already, during the war and especially after it, organized the departure of hundreds of young Islamic believers from the Western Balkans to religious education centres, with the aim that they would, upon return, become the transmitters of "true religion".

All of those who returned from studying, no matter whether they were previously practicing Wahhabism or were members of the Islamic Community, now preach Islam exclusively in accordance with Wahhabi teachings, giving a new impetus to Islamistic extremism in the Balkans (Bećirević, 2016).

The tendency of the growth of Islamistic extremism in Kosovo and Macedonia is closely linked with the sending of young people to Islamic studies and pilgrimage, or just longer stay in the countries – hothouses of religious radicalism (especially Saudi Arabia, Yemen, Malaysia and Egypt), from where they return as high quality propagandists of Islamistic extremism and become Islamistic priests or preachers who frequently change their place of living and hold lectures that attract great attention of the believers.

In Sandzak, an geographical area, administratively divided between Serbia and Montenegro, the former volunteers from the civil war in Bosnia and Herzegovina and students who had attended Islamic universities in Arab states, have all adopted the Wahhabi interpretation of Islam, but still in Sandzak, prevailing influence is that of radical Islamists from Bosnia and Herzegovina. The same aim is shared by radical Islamic sites calling for jihad (Lieberman and Collins, 2008) and advocating suicide attacks to kill Christians, such as the Internet site www kelimetal-haqq.org

The consequence of their extremist propaganda is the establishment of certain number of paramesdzads in private facilities in Sandzak. A strong connection between the extremists from Bosnia and Herzegovina and Sandzak was confirmed in 2011, when a Wahhabi from Sandzak attacked the US Embassy in Sarajevo (ICG, 2013; Novosti, 2011).

Characteristic for the way radical Islamists operate in Albania is the establishment of a number of institutes and centres where religious education of believers is conducted according to the Wahhabi Islamic teachings, which

are funded by Munazmat al-Islam, the most influential Islamic fund linked to Al Qaeda, and also by funds from Algeria and Kuwait.

Those who express dedication to this ideology and religious beliefs during the courses, are sent to higher levels of religious education institutions, most often to Islamic faculties in Saudi Arabia, Syria, Pakistan, Yemen and Egypt, where additional indoctrination is conducted, while some of them also undergo military training.

Those returning to Albania continue to spread jihadism and also represent significant support for Islamists with whom they had already established connections (Matoshi, 2001).

The emergence of jihadism in Montenegro is related to the import of Wahhabi ideology and its acceptance by extremists among the local Muslim population, concentrated mainly in the northern part of the state, in the municipalities which once were parts of Sandzak.

The Wahhabis from Bosnia and Herzegovina and Serbia had a significant influence on the occurrence and spread of Wahhabism in the north part of Montenegro, while the radical Muslims from Albania made a greater impact on the Montenegrin coast (Rakić i Jurišić, 2012).

In addition to that, the extent of the previous repulsion of Muslim believers in the Western Balkans towards Wahhabism has also been significantly reduced.

According to the IRI data from 2017, about 15% of the Bosnia and Herzegovina population approves Wahhabism, while 3% approve suicide attacks (IRI, 2017). According to the IOM (International Organization for Migrations) Regional Report on the vulnerability and resilience of local communities towards violent extremism from June 2017, the percentage of family participation in the Bosnia and Herzegovina in the process of radicalization is 6.61%, which is less than the usual percentage in Islamic environments (Atran, 2015), but is twice as high as in other Balkan environments (International Organization for Migration [IOM], 2017).

According to the western services, as well as the intelligence services of Macedonia, in 2013 there were more than 7,000 followers of the Wahhabi Islamic doctrine in this country (Simeunović and Dolnik, 2013).

The growing support for Wahhabists in the region can also be seen from the number of group members on social networks. As individual actors of Islamist extremism in the Western Balkans – the main promoters, preachers and religious teachers who spread religious radicalism, persons like Sulejman Bugari and Nezim Halilović-Muderis from the Bosnia and Herzegovina (Vecernje novosti, 2005), could be pinpointed, as well as their followers who have status of a formal or non-formal membership.

The individual actors of Islamist extremism in the Western Balkans are, as a rule, of modest social background. These are young people of poor financial status, from the suburbs of large cities or from the interior regions. They rarely complete more than secondary school education, unless they have studied at faculties of religious studies. They mostly do poorly paid jobs in the private sector and tend to turn to petty crime (Simeunović, 2008).

There is an obvious correlation between, more or less bad economic situation of the Western Balkan societies and the enlisting of individual actors of Islamist extremism. The unemployment rate, as an indicator of this situation, is highest in those areas where religious radicalism has the highest growth rate, such as the Bosnia and Herzegovina, where rate of unemployment among young people reaches almost 40%, and in Kosovo, where the unemployment rate is permanently high, despite the fact that Kosovo has attracted foreign investments larger than the other countries in the region.

While unemployment in Albania amounted to 15.3% in the period from 1993 to 2017, in Montenegro 17.29% in the period from 2002 to 2018, in Serbia 17.81% in the period from 2008 to 2017, unemployment in Bosnia and Herzegovina amounted to 42.65% in the period from 2007 to 2017, reaching up to 46.10%, and in the period from 2001 to 2017, it amounted to an average of 30.60% per year, reaching, in some years 57% (Trading Economist, 2018; Trading Economist, 2018a; Trading Economist, 2018b; Trading Economist, 2018c; Trading Economist, 2018d).

The reasons for the rise in the number of Islamic extremists in Albania are of a somewhat different nature. Recent research confirms that in Albania, a high percentage of respondents consider that Islam in this country affects the social and, more importantly, the private life of citizens (Cinar and Gonzalez, 2013), and that Islam has its own political institutions, which leads to the rise of Islamic extremism.

The supporters of extreme Islamist ideology in the Balkans now act in one of two factions: "neotakfir" and "reformers". The so-called fraction "neotakfir" acts through Wahhabi organizations whose objective is establishing a Balkan Islamist state by force – an emirate ruled by the Sharia law, which would include Albania, Bosnia and Herzegovina, Kosovo, Sandzak and Macedonia. "Reformist" fraction operates within the Islamistic Community of Bosnia and Herzegovina with the same objective, but advocates non-violent methods (Simeunović, 2016b).

A particularly high level of impetus to Islamist extremism in the Western Balkans, as in many other countries of the world, was given by ISIL's big successes in the war-torn areas of Iraq and Syria over the past decade,

resulting in an extremely large response from young extremists from the Balkans to enter this criminally -religious organizations.

There has also been a significant change, not only on the propaganda plan, but also in the leadership. While in the first years of the existence of Islamistic extremism in the Balkans, the main authorities were foreign mujahedeens, with the decline in their number and level of financial support, the leadership positions in paradzemates and radical groups have been taken over by Bosniaks and Albanians – Takfirs, which are considered the most aggressive Wahhabis i.e. Salafists (Baer, 2008).

Financiers: The first and the largest, and as it has been proven, permanent financiers of Islamistic extremism in the Balkans, were and still remain donors of numerous humanitarian Islamic foundations from Iran and rich Arab countries, primarily from Saudi Arabia, as the collective actors of Islamistic extremism.

Apart from them, Wahhabists and generally Salafia religious groups and communities, paradzemats and different cultural, sports and traditionalistic associations of citizens, and specialized non-governmental organizations can be labelled as collective actors of Islamistic extremism in the Western Balkans (Azinović, 2015).

Although these groups and organizations are not financiers of extremism, they act as a transmission mechanism for financing Islamistic extremism. During the last decade of the 20th century, these and similar foundations were also financiers of the terrorist activities of Al Qaeda and other Islamistic terrorist organizations, and because of these and other criminal activities were under attack from the international community, banned and their activists condemned to long term sentences (BBC, 2012).

However, after a certain period of time, these organizations renewed their work in the Western Balkans, working not only under the different, but also under the same names, often employing the same staff who used to work for similar organizations whose work had also been forbidden. Apart from the activities for which they are registered, these organizations are engaged in transmitting the Wahhabi-Salafi interpretation of Islam and, generally, the idea of Islamist radicalism.

The more important ones are: WAMY, Kuwait Joint Relief Committee (KJRC), Islamic World Committee (IWC), Al Waqf al-Islami Organization (WIO), Global Relief Mondial Service (GRMS), Revival of Islamic Heritage Society (RIHS), Islamic Youth Forum (IYF) and Bamirsia (Tok, Calleja and El – Ghaish, 2014).

These organizations operate through their branches throughout the Balkans, but not in the central Serbia, where no organizations or branches of this kind have been registered. However, these organizations do not operate only within the borders of their host countries. The example for that are Islamic cultural centres in Albania, whose activities strongly influenced the recruitment of young Albanians from Kosovo for jihad.

Moreover, the states which spread their own religion teachings are also the financiers of Islamistic extremism. While Iran was engaged financially in the late 80`s in Albania, and after that in Bosnia and Herzegovina, Saudi Arabia, is present today and was present in the past in Bosnia and Herzegovina and Kosovo. Jihadists in Macedonia are mostly financed by donations from Pakistan, but also from Saudi Arabia, Jordan, Syria and Iran.

Obviously, the attention of the international community weakened when it comes to funding Islamic extremism in this region. It can be concluded that, after the energetic reactions from the United States and other Western countries following September 11, 2001, the flows of financing Islamistic extremism in the Western Balkans were cut, but only for the short time, and were restored at the beginning of this decade (Sandić, 2011).

Al-Qaida and other terrorist organizations were and still remain the financers, which gave money to radical Islamists in the Balkans, with the aim to open the "third front" in this area. Al Qaeda sent money, not only to the extremists in Bosnia and Herzegovina, but also in Kosovo, while in Macedonia, Al-Qaida gave $ 7 million to the terrorist organization ONA and by doing this, at the same time, did "money laundering" (Taneski, 2010, p. 94). Al Qaeda`s links to Montenegrian Wahhabists were confirmed in 2007 when the Montenegrian police confiscated money and propaganda material, sent by the Taliban and Al Qaeda, on how to perform suicide and other terrorist attacks (Rakić i Jurišić, 2012).

Another permanent and growing source of funding Islamistic extremists` activities in the Western Balkans comes from different criminal activities of Islamistic extremists (CSSTR, 2011), mainly illegal drug trafficking, arms (Farnam, 2003) and human trafficking (Brisard, 2002). These activities lead to the creation of a hybrid profile of extremist organizations and groups which are not any more only political-religious, but become criminal organizations also. This phenomenon is, in theory, called narcoterrorism.

An example for this is ANA (Albanian National Army), which was, at the time, simultaneously put on two lists in the United States – as a terrorist and also as a criminal organization. While, in 2003, UNMIK proclaimed ANA a terrorist organization, because it was more Islamistically oriented than the

KLA, and this was completely in line with the advanced process of extreme Islamization of the Balkans (Matoshi, 2001).

In Montenegro, the extremists receive money mainly from Islamistic organizations, but also from drug smuggling. Proof that these funds are aimed at spreading Islam is an increasing number of newly built mosques, so when it comes to the number of mosques in relation to the number of inhabitants, Montenegro has the highest rate in the region (Islam Montenegro, 2011).

The term "Islamistic Network" which has been used increasingly in the criminalistics to mark various forms of illegal trafficking in an area from the Middle East to EU countries, also includes criminal activities of fundamentalist religious circles from the Western Balkans, primarily from Albania, Kosovo, Macedonia, Sandzak and Bosnia and Herzegovina, which include "heroin smuggling from Afghanistan by the Talibans and Al Qaeda" (Makarenko, 2004, p. 132), and in recent years, also by the Kurdish PKK (Dikici, 2008; Simeunovic and Dolnik, 2013).

In Macedonia, the Pakistani missionary movement Tablig Jemath (Jamaat Teblig) occasionally smuggles weapons. In recent years, Sandzak has become an important link with drug cartels, although Kosovo is in the forefront of it. In 2004, the FBI launched a comprehensive investigation into the links between the Albanian Islamic Network and international terrorist financing (Frieden, 2004).

Objectives and methods of action used by extremist Islamic believers in the Western Balkans

Objectives classification: The objectives of extremist Islamic believers in the Western Balkans can be classified, according to their significance, to historical, strategic, tactical and operational goals. The general goals of their fight include historical and strategic goals, while the goals of particular groups or organizations of Islamistic extremists in the Western Balkans include operational, tactical and most of their strategic objectives (Simeunović, 2009).

The historical goals of Islamistic extremists in the Balkans are the most important ones and, at the same time, the most comprehensive, while the moment of their achievement is located in the far future. The basic historical goals of all the groups and leaders of Islamistic extremism in the Western Balkans are to impose Islam as the one and only world religion and to create ummah, a world state and society that would include all the Muslims in the world (Fares, 2008).

The strategic goals are more numerous and their implementation should lead to the achievement of the already set historical goals. These include: the spread of a radical version of Islam, the mass enlisting of followers into Wahhabi teaching, the formation of combat organizations, the unification with all similar Salafi groups and movements, the self-identification of masses with the actions of radical Islamists, the liberation of the "enslaved brothers" in other countries and contribution to global jihad by personal participation.

The main strategic goal of all Islamistic extremists in the Western Balkans is the creation of a Balkan emirate, caliphate or vilayet (depending on the expression used by different preachers in different communities), which do not have the same meaning, but could be, in the end, defined as a kind of Balkan religious state that would include Albania, Bosnia and Herzegovina, Kosovo, Macedonia and Sandzak, meaning not only Sandzak`s part in Serbia, but also a part of the territory of Montenegro.

The proof that the strategic goals of the Islamistic extremists in the Balkans do not have necessarily to be identical in all communities, is shown by the territorial pretensions of Islamistic extremists in Macedonia, which are not limited only to the territory of that state, but, as the former chief mufti of Bulgaria, Nedim Gandzhev`s statement confirm, these extremists tend to create a fundamentalist triangle between Bosnia and Herzegovina, Macedonia and the Western Rhodope Mountains in Bulgaria. (Deliso, 2007).

In the operationalization of the goals of Islamistic extremists in the Balkans, tactical goals are those which lead to the actualization of the strategic ones and from which they are derived as their important segment. For example: performing concrete actions of "retaliation" with the aim of weakening the power of their opponents, strengthening their positions in a particular community, establishing of paradzemats, performing various concrete actions with the aim to improve the number, personnel and financial reinforcement and the use of mass media to propagate their ideas and mobilize membership.

As operational ones, specific individual goals of the lowest level of generality can be determined, because they are substantially exhausted at the level of tactical concretization. So, for example, concretization of the "retaliation" as a tactical goal of Islamistic extremists in the Western Balkans includes the realization of the following operational goals: attack on facilities of political significance, attack on church facilities, direct strike "in the heart" of the state by murdering persons on high political, police or military position, causing anxiety of life among citizens of other religions by periodic violence

etc. (Azinović, 2015; Bardos, 2005; Deliso, 2007; Hamad, 2007; Shay, 2008; Simeunović i Dolnik, 2013).

Contents and methods of operation: Despite the initial mistrust of Islamic believers towards Wahhabis, and their frequent confrontations with official Islamic communities in the Balkans, Wahhabis managed to maintain a presence in this area, due to the money which they received from Saudi Arabia and other donor countries (Sandic, 2011). This is very important, bearing in mind that Western Balkan societies are impoverished, and, as we have noted, the unemployment rate in some of them is extremely high (Trading Economist, 2018).

Wahhabis activities range from the ordinary or permissible religious activities like building their own places of worship in the Western Balkans (Islamic Community of Montenegro, 2011; Islamic Community of Bosnia and Herzegovina, 2015) in order to create as distinctive pro-Islamic atmosphere as possible, spreading their teaching of Islam through lectures, books, by creating websites and the use of social networks on the Internet in order to attract new members (Kosovar Center for Security Studies [KCSS], 2018), to aggressive actions such are taking over by force the mosques which are under the jurisdiction of the official Islamic Communities in the Western Balkan countries, spreading hate speech of religious and national animosity (Vecernje novosti, 2005), recruiting volunteers to go to the Middle East battlefields in order to join terrorist organizations, like ISIL and Al Nusra in the first place, and persuading individuals and groups to carry out terrorist activities in a domicile country or surrounding areas, and more and more lately on the US and the EU territory (Selimi i Stojkovski, 2016; Simeunović, 2012, 2014).

For these purposes, Wahhabis set up camps in the region, to provide the paramilitary training, based on Islamic military tradition, for their members. In order to attract young people, who are their most important target group, they organize, in big cities, courses not only in Arabic, but more and more lately in English language, and also different computer courses for young population. In Kosovo, one radical preacher set up TV station called "Peace TV", on which the ideas of Islamistic extremism are constantly very aggressively propagated, hate speech spread against not only non-Muslims, but also against Muslims who do not accept Wahhabism, and bin Laden is glorified (Al-Alawi, 2012; Utrinski vesnik, 2010). One of the Islamistic forums, in 2010 for the first time in Albania, broadcasted a song dedicated to bin Laden (Utrinski vesnik, 2010) in Albanian language, and since then, religious extremism has been extensively spreading in Albanian, as well as in Bosniak language. Also, so called Islamic State publishes some of its materials, not only

in four major world languages and Arabic, but also in Bosniac and Albanian Telegraf, 2017).

One important and more and more lately widespread content of Wahhabis work in the Western Balkans, has been the swift establishment of the network of settlements called paradzemats, atypical not only for Europe but also for the Balkans, in which they live with their families, not practicing the laws of the local state, but Sharia law and educating children using religious teaching programs. In mid-2015, the Islamic Community of Bosnia and Herzegovina reported that there are 64 paradzemas in Bosnia and Herzegovina under the absolute control of the Wahhabis (Vecernji list, 2016, Islamic Community of Bosnia and Herzegovina, 2015), comparing with the few years before, precisely 2011, when there were only four paradzemas. In Macedonia also, the Mujahideen organization called Tablig Dzemat set up several paradzemats and camps (Deliso, 2007). The largest number of paradzemas camps is placed in Kosovo, in former training centres which were used by KLA (Simeunović, 2009). Wahhabis' activity in Montenegro is characterized by gatherings in the camps in Plav and in the border region with Kosovo, attended by Islamists from the country and the surrounding areas (Rakić i Jurišić, 2012).

According to the statements of extremists published in their public media, the formation of the so-called Islamic State on the ground of Iraq and Syria has inspired the Islamistic extremists to try similar attempt in the Balkans, to establish a "punctate caliphate" composed of a network of linked paradzemats, usually not territorially interconnected, with the tendency of further growing until this "Balkan Emirate" does not include, apart from Bosnia and Herzegovina, the Raska-Polimlje region, Kosovo, Macedonia and Albania (Allah's grace 2013).

Methods of Wahhabis work include increasing abuse of democratic mechanisms of social and political activity, such are the establishment and operation of non-governmental organizations, cultural societies, religious sport societies and traditionalist associations (Azinović, 2015), whose proselytism leads to illegal activities such are organizing the departure of extremists to the battlefields, a drastic restriction of women's rights, abuse of the Internet and the media with the aim to spread hate towards members of other religious communities and glorifying Islamic terrorist activities as ethically and religiously correct.

Also, some paradzemats, like Teblig in Macedonia in 2001, organized and sent their members into armed conflicts between Albanians and Macedonian security forces (Deliso, 2007). In this way, it is again confirmed as correct, the thesis about the relation between terrorism and democracy, in

terms of creating increased possibilities for concealed extremist gathering and activities due to the existence of a number of democratic rights and freedoms (Wilkinson, 2002).

In all the countries of the Western Balkans, there is an increase in the activities of Islamistic extremists, which is neither so fast nor as dramatic as it is sometimes presented in the media, but definitely it is constant. The highest level of increase is in Bosnia and Herzegovina, Kosovo and in Macedonia. The characteristics of Islamistic extremism in Bosnia and Herzegovina are paradzemats, which are far less widespread in other Balkan areas, while the characteristics of the Islamistic extremist milieu of Kosovo is a mixture of nationalistic, extremist religious and criminal activities all taken by the same individuals and groups. In Macedonia, there is a specific insistence of Islamistic extremists on the actions of the masses which lead to a deep religious, not just ethnic division of Macedonian society.

The Islamistic extremism of the Western Balkans as a regional and global security challenge

Participation in global jihad: The activities of Islamistic extremists with which, they think they contribute to the global jihad are mainly taking place in three fields: the conduct of terrorist actions in the Balkans, the joining of Islamistic terrorist organizations such are ISIL, Al Nusra, and earlier Al Qaeda, and in the execution of "homegrown" terrorism acts on the territory of "hostile countries" such are the US and the EU countries. The conduct of terrorist activities in the Balkans by Islamistic extremists can be described as periodic but constant. All this is a logical consequence of the degree of development of the Islamic radical population in the Balkans and its traditional determination to fight for its goals by using violence. The latest trends in the activities of the Balkan Islamistic extremists are the departure for the Middle East battlefields and there, although in fewer numbers, participation in the "home-grown" extremist activities on the territory of the EU and the USA (The New York Times, 2009; Simeunović, 2014; Thachuk, Bowman and Richardson, 2008).

The number of volunteer fighters from Serbia who are on the Iraqi or Syrian battlefield is 28, including two women. Eleven of these fighters were killed, while ten returned to Serbia. Three of them were arrested and are waiting for a trial, three escaped to Kosovo, two went to Austria, and one person was arrested in Greece where he had come from Sweden. Most of them left Serbia and went to the battlefields in 2013 and 2014 through the territory of Bulgaria and Turkey. By the end of 2016, another five new departures for

the battlefields (Simeunović, 2016) were recorded. In the period from 2012 to 2015 only, 314 volunteers from Kosovo departed to fight for ISIL and Al Nusra (Azinović and Jusić, 2016).

It is assumed that the total number of Bosnia and Herzegovina citizens who fought in the Middle East battlefields, in the period from 2012 to 2017, was 286 persons, although Bosnia and Herzegovina officials also mentioned different numbers that ranged up to 350. During 2016 and 2017 there were no recorded departures, but two attempts of departure were prevented, one in 2016 and one in 2017, so it can be said that the trend of departure of Bosnia and Herzegovina citizens to the battlefields had almost stopped, which was mainly due to the defeat of so-called Islamic state. (Azinović and Jusić, 2016)

The number of Islamistic extremists who left Macedonia to fight in the Middle East in 2015 amounted to about 150 (Azinovic and Jusic, 2016). While this figure, according to the statement of the President of Macedonia, George Ivanov, fell to about 110 in 2016, because 25 of these fighters were killed and 86 returned to Macedonia (Selimi and Stojkovski, 2016). The reaction of the Macedonian authorities to the departure of its citizens for foreign battlefield resulted in police operations in 2016, when twenty people were arrested, and the key organizer of the volunteers` departures to the Middle East militias, a radical imam, was sentenced to seven years in prison (Selimi and Stojkovski, 2016).

Over the past five or six years, Islamistic centres in Albania, which are the main centres for recruiting young people for jihad, sent around 150 extremists from Albania to the Middle East to join ISIL (Simeunović, 2016) and different Al Qaeda affiliates, such as Džabat Al Nusre, but due to the possibility of the influence of various informal groups, this estimation can rise up to 200 (Tadić, 2017).

The jihadist trend of departing for the Middle East battlegrounds did not overlook Montenegro. The presence of Wahhabism in Montenegro resulted in about 40 volunteers from Montenegro, between 2012 and 2015, (Azinović and Jusić, 2016) joining the Middle East forces, among them a few women.

The Islamistic extremism began to manifest itself in the field of suicide terrorism. The first suicide bomber from the Balkans was a Kosovo Albanian who committed a terrorist act in Iraq at the end of March 2014, killing 52 people (Svetinje Braničeva, 2014). The suicide acts of other Balkan jihadists, which followed afterwards, proved the readiness of the Balkan extremists to commit suicide attacks, although experts had been expressing doubts about the possibility of such attacks for a long time.

In the last few years the number of local extremists departing for the Middle East battlefields, had declined, firstly, due to the adoption of the legal

measures in all Western Balkan countries against participation of their citizens in wars on the territory of foreign countries, and secondly, due to the defeat of so-called Islamic State. Therefore, the main security challenge of Islamistic terrorism in all Western Balkan countries remains the possibility of occasional terrorist incidents and the activities of returnees from the Middle East conflict.

Influence in the country and abroad: Although it has long been known that the main sources of extremism in the Balkans are Wahhabist centers (the Islamic Community of Bosnia and Herzegovina, 2015, the Islamic Community of Montenegro, 2011), Islamistic extremism is not only present in the Wahhabi communities as it is commonly thought, since a quarter of a century long presence of Wahhabism in The Balkans has proven that not all the Wahhabis are extremists, as it also shows that not all the members of the official Islamic communities in the Balkan countries have been immune to extremism any more. Given that of the fact that a slow, but stable increase in the number of supporters of Islamistic extremism as well as a growth of their activities in the Balkans and the world, especially in the Middle East and the US and the EU has been observed, the Western Balkans have been marked, not only by a number of authors, but also by representatives of the international community, as one of the "black spots" with regard to the human resources base and logistics of Islamic terrorism (Archick, Rollins and Woehrel 2005; Shay, 2008). The growing influence of violent and expansive extremist Islamistic ideologies in the Western Balkans is a serious security challenge not only for the Balkan and the surrounding countries, but also, through the realization of "home-grown" terrorism connected with the Balkan, increasingly for both the EU and the US (Simeunović, 2012).

In Macedonia, the emergence of Islamistic extremism and terrorism is closely linked with the factors that have already demonstrated their influence in Bosnia and Herzegovina, Albania and Kosovo (Babanovski, 2002; Panovski, 2011; KCSS, 2018; Selimi and Stojkovski, 2016). Terrorism in Macedonia finds its source not only in the ideology of extreme Albanian nationalism, but also in religious exclusiveness. The violence of Albanian extremists that has been destabilizing Macedonia since 2001, turning the country into a state of permanent crisis, consists not only of ethno-separatist tendency but also of radical religious-Islamic dimension, whose source comes from jihad postulates (Grizold and Zupancic, 2008).

The reactive nationalism which emerged among the Christians in Macedonia only makes the situation worse, affecting the security of the entire region. A significant security threat is posed also by the actions of the Wahhabi

groups from the South of Serbia, whose aims of Islamistic extremism and separatism are merged together (Huszska, 2007). These groups, which sent almost half of total number of fighters from Serbia to the Middle East war, also pose a threat because of their close ties with extreme Wahhabis in Kosovo, Macedonia and Albania. The activities of radical Islamists in Albania are characterized by the establishment of several Wahhabi institutes and centres that intensively gather radical Islamists from all over the region and therefore represent a security risk for the entire region. Today, even Albanians themselves consider that Albanian political Islamism poses a threat to the Western countries (Cinar and Gonzalez, 2013).

However, this does not apply to Albania itself, where, unlike neighbouring Kosovo or Macedonia, despite the Muslim majority, there is a tradition of mutual tolerance towards the citizens of other religions (Babuna, 2003). The reason for this is the religiously homogeneous society in Albania, mostly inhabited by Albanians (95%), with insignificant percentage of minorities. The situation in Montenegro is specific, not only because the Wahhabis are numerous and deeply rooted in some cities with the Muslim population in Montenegro, while not present at all in others cities, but partly because of the extreme activities of the Albanian Catholics, who formed a terrorist organization (B92-Vesti, 2007) with the aim of threatening primarily Muslims in Montenegro. The radical Catholics claimed that Muslims they have much more rights than the Catholics in this country.

The ISIL or Al Nusra returnees pose a threat to the entire Western Balkan and the surrounding countries, since after participation in the fighting; they became case-hardened terrorists. When they had set off to the Middle East, most of them were not really dangerous, they were mainly religious fanatics, without any combat experience, and as such, on arrival to the battlefield, often got killed in their first battles, like other new fighters. However, those who survived the Middle East war hell, are those who probably had carried out a series of terrorist acts and killed certain number of people, which means they can be viewed as people with a high capacity for destruction. A significant risk of their return lays in the fact that, after the return they become "heroes" and great examples to young people in their surroundings. For example, the Bosnian salafists who carried out terrorist attacks in Zvornik and Sarajevo in 2015 had been, before committing the acts, in contact with returnees from the Syrian war zone for months (Azinović, 2015).

Taking into consideration that returnees from the Middle East battlefields could face legal charges and long prison sentences in all the Western Balkan countries, it can be expected that they will not return in

greater numbers to their home countries, but some of them will remain in the Middle East, while others will use migrant or some other routes to reach the EU countries, which increases the risk of "home-grown" terrorism in these countries, and requires extra caution regarding organizations and individuals who have or have had contacts with extremists. For that reason, the Bavarian Service for the Protection of the Constitutional Order confirmed in 2017 that the KLA is on their list of militant extremist organizations (B92-info, 2017), although this organization was formally dissolved a long time ago.

The radical Kosovo Islamists, who have become particularly militant over the past few years, are increasing the "home-grown" threat to America and the EU (Lieberman and Collins, 2008), like in 2007, when several Albanians arriving from Macedonia and Kosovo planned to kill the president of the United States and the US soldiers at Fort Dix, or in 2011 when an Albanian from Kosovo killed two US soldiers at the airport in Frankfurt (Simeunović, 2014). The gravity of their intentions and actions is indicated by the fact that all of them were sentenced to life sentences in the US and German courts (Stars and Stripes, 2012).

The ability of Balkan societies to combat the Islamistic extremism

Characteristics of combating Islamistic extremism: The aim of this section is not to carry out a comprehensive analysis of the capabilities of each Western Balkan country to confront Islamistic extremism, but to determine certain characteristics of each of them in this field. There is almost no high-quality prevention against Islamistic extremism or successful de-radicalization in Bosnia and Herzegovina, but mainly, the uneven, repressive practice towards the extremists is implemented (Southeast European Times, 2008).

One of the reasons for that, could be, according to the statement of Sredoje Novic, the Minister of the Government of the Federation of BiH, "that in the political structures of Bosnia and Herzegovina there are a certain number of individuals who are not only prone to extremist ideas, but also belong to such organizations" (B92-info, 2015). Because of the insufficient confrontation against Islamistic extremism, Bosnia and Herzegovina and its institutions constantly come under criticism of leadership and high representatives of international institutions and organizations.

Kosovo, despite all the efforts of EULEX and other international institutions to create rule of law and legal system in it and liberate Kosovo from organized crime and rising extremism, failed to get out of poverty and high unemployment rate, despite the fact that in the last couple of years it has attracted the largest foreign investments in the Balkans. The social poverty

and still relatively poor education level of the population considerably ease the spread of Islamistic extremism, because of the fact that together with its inflammatory ideas always goes some money. The statement of the UN Secretary General at the beginning of 2018, that Kosovo had regressed in all aspects, became part of the UN document on February 17, 2018.

In the framework of the prevention of Islamistic extremism and organized crime in Sandzak, Serbia strategically started to cooperate with Turkey, a country with a traditionally strong influence on Bosniaks. Because of promoting moderate Islam, Turkey is considered as an important factor in combating Wahhabi extremism in the region. In Albania, the situation in terms of the capability to confront Islamistic extremism has improved since Albania joined NATO, which provides this country with considerable assistance in this regard.

Albania's efforts to distance itself from Islamistic extremism are certainly helped by the developed traditions of mutual religious tolerance because of its religiously homogeneous society (Babuna, 2003). These efforts are being hampered by the fact that the process of restoring religiosity in the whole Albanian society is still massive.

For the sake of prevention, Montenegrin police, have been announcing in the media that it observes the Wahhabi centres and prominent individuals, and their contacts with the Wahhabis from Sandzak (Dan online, 2012). According to the assessment of the Police Directorate and the National Security Agency of Montenegro there are about 150 Wahhabis in that country, and according to other sources, this number is larger and could rise to 200 persons. Until recently, the authorities of Montenegro largely denied the presence of Wahhabism in their territories, or were silent about it, fearing that this could impede their entry into NATO.

The attitude of Islamic communities in the Western Balkans toward Islamistic extremism: The Riaset of the Islamic Community of Bosnia and Herzegovina, under the threat of Wahhabism, has distanced itself several times from Wahhabis, but mildly, without openly mentioning Wahhabism. Instead, formulations like "inadequate aggressiveness of individuals and groups in the interpretation of Islam, which is upsetting Muslims" were used (Islamic Community of Bosnia and Herzegovina, 2015). The most important measure taken by the Islamic Community of Bosnia and Herzegovina was the Resolution on the interpretation of Islam, adopted by Rijaset in March 2006, whose formulation was very mild and unclear. Furthermore, following requests from representatives of the international community, the Reis of the Bosnia and Herzegovina in 2016 launched an

action aimed at integrating paradzemats into the Islamic Community of the Bosnia and Herzegovina.

In Sandzak, the existence of Wahhabi had been denied until 2007, but even before that, the local religious Muslim leaders had often complained that the extremists had terrorized them and accused of betraying Islam. According to the ICG (International Crisis Group) report of 8 April 2005, Wahhabis had already controlled by force several local mosques in Sandzak. Since then, the Wahhabis have begun to act more and more aggressively, causing numerous incidents in local mosques and public places, trying to, like they did in Bosnia, Macedonia and Montenegro, take over, primarily by force the mosques of the Islamic Community in Sandzak. With that in mind, they have made numerous attacks on the official imams and their supporters.

Like in other parts of the Balkans, in Macedonia also, Wahhabi and Salafi factions funded by Islamistic organizations are constantly in confrontation with traditionally moderate local Muslims. From 2003 to 2006 the Wahhabi was extremely aggressive, and in that period, "in Macedonia there were numerous incidents in which they were taking leading part. In particular, their aggressive behaviour towards other imams from the Islamic Religious Community of Macedonia was evident." (CSSTR, 2007) Later also, a number of aggressive attempts were made to gain control over mosques by Wahhabis, but from 2010 in Macedonia, numerous mosques have been taken over by radical groups, in forced and unlawful manner (CSSTR, 2011; Öktem, 2010). The specificity of the Islamic Community of Macedonia, comparing with the other Islamic communities in the Western Balkans, is that it has been increasingly under the influence of the radical Wahhabi imams since the mid-1990s, and that they, today, dominate its leadership.

Since taking over of mosques became a form of Wahhabi activity in the Western Balkans, the same pattern was applied in Montenegro, where the Wahhabis took control of certain mosques and physically hurt imams. The Reis of the Islamic Community in Montenegro has warned, several times, that Wahhabis justify terrorist actions and call followers to jihad.

The Islamic Community of Montenegro took very similar measures against Islamistic extremists (also with little effect), like Islamic Community of Bosnia and Herzegovina, condemning the "aggressiveness of individuals and groups in the interpretation of Islam" and their physical and verbal attacks on followers and officials of the Islamic Community, but without mentioning Wahhabism (Casoli, 2007).

Conflicts between the the Islamic Community of Serbia and the Islamic Religious Community of Montenegro in 2014, have helped the Wahhabi to boost religious activities within private masjids and mosques which are not

part of the Islamic Community's system, and because of these conflicts, Wahhabi managed to attract new followers, especially young people.

Conclusion

Islamistic extremism, as a wide fertile soil for the most important modern type of terrorism, is not losing its battle against the leading democratic orders as considered by most of the authors today, but only suffers from occasional defeats, in order to re-emerge, not giving up, at any moment, violence as a mean of achieving its goals. The proof of Islamistic extremism`s vitality is the persistent and systematic spread of its ideology and the constant increase in the number of its sympathizers around the world, despite all the efforts of the international Community. Even the Balkan countries, with bigger or smaller percentage of native Muslim population, did not escape that trend. These countries, known under the name of the Western Balkans, are Albania, Bosnia and Herzegovina, Montenegro, Kosovo, Macedonia and Serbia.

By analyzing the causes of the emergence of Islamist extremism, the factors of its survival and growth, as well as detecting main individual actors and extremist organizations, leads to the conclusion that the Islamistic extremism has been present, but not continuously, in the recent history of the Balkans especially during the wars, but that the Balkans for the last quarter of a century has become a fertile ground for non-traditional religious ideologies and religious-political movements such as Wahhabism and that Islamistic extremism is now continuous and very present in all the Western Balkan countries, not only in Bosnia and Herzegovina and Albania, as it was two decades ago.

The main contribution of this paper is that, unlike the rest of existing literature on the subject, it determines that the rising trend of Islamistic extremism in the Western Balkans and, in particular, the growing number of its followers, is caused by several factors, ranging from unhealed interethnic tensions that are always religious in origin, a new wave of "domestic" preachers of extremism trained in Islamic countries, the restoration of the presence and the financial support of Islamistic humanitarian organizations, to the inevitable reflections of the Middle East wars that cause emotional reactions of a certain number of Balkan Muslims in the spectrum from empathy to the perpetration of terrorist violence in the Balkans, the US and the EU countries, and in the units of terrorist organizations in the Middle East, all for the revenge of suffering of their co-believers.

The new big incentive to Islamistic extremism around the world, also in the Western Balkans, was ISIL`s attempt to build an authentic

fundamentalist Islamistic state in the war-torn territories of Syria and Iraq. Also, the lack of good governance in the Western Balkan states has contributed significantly to the growth of radical Islam in these countries (Tadić, 2017).

An insight into the goals, methods and contents of the work, and the types of activities of the actors of Islamistic extremism in each of the analyzed societies in the Western Balkans, where Islamistic extremism is present, makes it possible to conclude that, with full respect for the literature offering evidence for the differences in the manifestations of Islamistic extremism in each of these particular societies, Islamistic extremism in the Western Balkans must be treated as a unique political and religious phenomenon.

This assessment has been obtained not only from the fact that they have identical goals, inspirers and foreign financiers, methods and contents of their work, but also from the close connection and frequency of contacts between Islamistic extremists from all Western Balkan countries and their joint participation in various activities such as religious lectures, gatherings, training, armaments, financing of mosques and other joint projects, but also their cooperation in the planning and execution of terrorist actions. The most important thing they have in common is jihadist ideology and the readiness to achieve its postulates by force, even at the cost of their own lives.

The main goal of Islamistic extremists in the Western Balkans is the building of an Islamic society and the formation of its own government based on Sharia law in the merged areas of Albania, BiH, Montenegro, Kosovo, Macedonia and Sandzak. For this purpose, the embryo of the projected future Balkan caliphate is created as punctate network of extremist settlements and paradzemats. This network, for the time being, is mostly widespread in Bosnia and Herzegovina, which is the main regional hotspot of Islamistic radicalism, with the tendency of spreading its network to the other countries in the region.

The swing of Islamistic extremism is obvious from the fact that, besides Bosnia and Herzegovina, traditionally a main regional centre of Islamistic extremist activity, with the passing of time, Kosovo has become the "black dot" on the map of Islamistic extremism in Europe. The proof for this is the number of Kosovo Albanians who went as foreign fighters to join terrorist organizations in Syria and Iraq. In Serbia, Montenegro and Albania, the current state of the threat of Islamistic extremism can be assessed as still bearable, whereas Macedonia, due to the growing religious-ethnic tensions and accelerated radicalization of one part of Islamistic believers, is in danger of becoming the third major hotbed of aggressive fundamentalism on Balkan.

The connections between radical Islamists from Kosovo, southern Serbia, Albania and Macedonia are a bit stronger than ties they have with

Islamists soul mates from Bosnia and Herzegovina and Sandzak, while radical Islamists from Bosnia and Herzegovina have the strongest ties with their soul mates from Sandzak and Montenegro. This leads to the conclusion that it is possible to speak about two action areas of Islamistic extremism in the Western Balkans. In addition, this division should not be seen as an intentional strategy but rather, as a consequence of language differences of the Balkan Islamists of Slavic and Albanian origin that, because of their relatively low level of education and knowledge of foreign languages, are hampered from more intensive mutual communication. However, Sandzak is the core that connects them all.

As a new tendency in Islamistic extremism in the Balkans, it can be noted that the extremism can no longer be equated with Wahhabism, nor extremists are found only in the Wahhabi communities, but extremists are almost equally present among the believers from the official Islamic communities in the Balkan countries. The reason for this may lay in the fact that the extreme Wahabites and Islamic communities in the Western Balkan countries are financed by the same countries and the same donor organizations.

Not only the islamization itself, but also the criminalization of extreme political, primarily nationalist movements and organizations, due to their increasing participation in organized crime, such as drug smuggling, human and weapons trafficking, led to the creation of hybrid criminal-religious-nationalist organizations and groups, on the territory of Kosovo, Albania and Macedonia in the first place, but even more, in Sandzak, Bosnia and Herzegovina and Montenegro. The new trends and characteristics of the West Balkan Islamistic extremism include the positioning and the firm organizing of radical Islamists in large cities where Muslims are not a significant part of the population, like in Belgrade, and also an increasing percentage of Roma and converts to Islam who take part in terrorist activities.

For Islamistic extremism in the Balkans, it is characteristic that statistically looking, a percentage of the family role in religious radicalization is relatively low, comparing to the other communities with this phenomenon. This can be explained by the absence of extremists in previous generations, but this percentage is steadily rising, and in Bosnia and Herzegovina is the highest.

Along with the growing presence of Wahhabism in the Western Balkans, not only the number of their organizations and members, paradzemats and settlements rise, but also the number of terrorists from their ranks, and also from the ranks of their followers living in the Diaspora, which altogether results in an increasing number of "home grown" terrorists who

originate from the Balkans, and who present a threat to citizens and goods of the US and the EU countries.

The fact that about a thousand volunteers (65% of whom are Albanians) from the Western Balkan countries joined the terrorist organizations like ISIL and Al Nusra must be a cause for worry. Therefore, the level of caution and prevention must be much higher than it has been up to now, regarding the elimination of Islamistic extremism from Western Balkan societies, not only because of the possible return of the terrorists to their homelands, which would give a new impulse to radicalization, but also because, obviously, in the Western Balkan countries nothing much has been done so far, about the prevention of Islamistic extremism and de-radicalization of its actors and sympathizers.

The situation is further complicated by the mass migrations from the Middle East and Africa that have plagued Europe over the past few years. Taking into account that almost all migrants are Muslim, there is a real possibility that Islamistic extremists are infiltrated and hidden in their ranks, though not in large numbers.

It is evident that the rising threat of Islamistic extremism in the Western Balkans is accompanied not only with the lack of genuine and high-quality prevention, inexperience and poor results regarding the deradicalization of extremists, but in some areas, with the lack of political will as well as the ability of the official Islamic communities to fight against Islamistic extremists more decisively. All above-mentioned together implies not only intensive cooperation between the police and other security structures of the states of the West Balkans and the countries in their surroundings, but also the urgent help of adequate institutions of the international community, first of all, the competent EU bodies.

Although being a general threat, the Islamistic extremism requires an approach that should be adapted to each particular community, while being led from the same centre. The EU's foreign and security policy strategy demands an approach that must be based on a full understanding of the local characteristics and on the creation of a wider and lasting regional framework for cooperation in that regard. The growth of Islamistic extremism in the Western Balkans and its manifestations requests urgent measures, such are the mandatory exchange of information between national police forces and Interpol and Europol, proactive cooperation with the European Counter-Terrorism Centre and the Police Cooperation Common Centres, the implementation of the conventions like the Police Cooperation Convention for Southeast Europe and stronger joint action on the border control (RECOM, 2017).

The abuse of the Internet for extremist purposes should be hindered with the help of specialized EU institutions such as the EU Internet Forum. Particularly important are the timely, organized programs for deradicalization, rehabilitation and reintegration of the extreme Islamists into the normal social flows. For this purpose, NGOs and local communities should be engaged, as well as the prominent influential individuals and groups, and cooperation should be fostered with European bodies such as the Radicalization Awareness Network (RAN) in order to stop the further impact of radical religious ideology in the societies of the Western Balkans.

The sustainable prevention of radicalization requires a comprehensive approach that takes into account the socio-economic situation, and especially the necessity of reducing the youth unemployment rate. In general, any form of supporting activity from the EU through initiatives like the Western Balkans Counter Terrorism Initiative and Integrative Internal Security Governance (IISG) is more than necessary (WBCTi, 2017, IISG, 2017).

It is encouraging that WBCTi and partners have already shown the necessary synergy by working on several new and useful solutions for the countries of the Western Balkans in order to eliminate the shortcomings in their strategic, political and operational cooperation so far, and also because of the introduction of new and improved standards. In this regard, particularly important and inspiring for further cooperation is Prevent-Refer-Address (P-R-A) concept derived from the WBCTi platform, which has been developed intensively in the region since 2016 as a part of the "First Line" project under the guidance of the Slovenian Ministry of the Interior (WBCTi, 2017).

The P-R-A concept includes the involvement of all the competent bodies at the national and local levels, including those that have not traditionally been involved in counterterrorism, i.e. educational and health institutions, civil society and non-governmental organizations, academic communities, religious communities, prisons and local communities, state authorities responsible for strategic communication, Ministry of Labour and Social Welfare, ministries responsible for culture, youth, sports, etc.

This concept also implies two-way instructions – firstly, instructions developed at the state level, according to relevant EU, regional and international standards and sent to practitioners at the local level who are dealing with concrete cases of radicalization and violent extremism in order to support measures they take in early prevention: and secondly, feedback information from these local experts send to the state level about deficiencies and good practices.

Furthermore, good effects are achieved by establishing effective and coordinated procedures for early prevention in the local community, and by

timely development of skills and abilities to cope with the existing and every new radicalization *modi operandi*; this implies optimal use of existing state and local structures, also the EU and international platforms, including national coordination structures, structures established within P/CVE national strategies; the transfer of knowledge of the RAN (The Radicalization Awareness Network – RAN) of the Emergency Situations Centre of the EU and the existing RAN networks focused on different sectors.

Within the P-R-A concept, the academic community has a special place through its research, to identify the most sensitive areas of violent extremism in the Western Balkans region, conducted by a consortium involving the most relevant research institutions with a specially developed methodology; which all together implies identifying synergies within the WBCTi and selecting the sustainable solutions (IISG, 2017; WBCTi, 2017).

From the findings of this paper, and according to the results of the previous engagement of the relevant institutions and initiatives to combat violent extremism, it can be concluded that there is a clear need for the far greater cooperation between the countries of the Western Balkans in the fight against Islamistic terrorism than before, and in order to have more successful results in combating Islamistic extremism and terrorism in the Western Balkans, there must be urgent move toward the maximum intensification of cooperation between the police and other security structures of the Western Balkan and the countries in their surroundings, all in coordination with the relevant institutions and bodies of the EU and other international actors.

Apart from strengthening the security information flow and developing its stability as an essential prerequisite for the successful fight against extremism and the mutual adjustment of legal measures to combat terrorism as primary tasks, also, an intensive organized social work on the protection and promotion of basic democratic values is essential, a comprehensive and legally regulated prevention of all aspects of religious intolerance, as well as much more fundamental scientific and professional dealing with the causes of extremism in the Balkans so that it can be eliminated as efficiently as possible. It is, also, necessary to adopt not only the latest international legal standards in the fight against extremism and terrorism, but also technological innovations developed for this purpose (Đurđević, Stevanović, Mitic and Kocić, 2016, p. 55; Mitic, Kocić, Tidrow and Fecht, 2017).

It is very important to realize, as soon as possible, that avoiding facing the truth and the reality about the degree of presence and the prospects of the advancing of Islamistic extremism in the Western Balkans, and not taking appropriate measures against it, allegedly in the name of good inter-faith or

interethnic relations, deteriorates the fight against Islamistic extremism as an global enemy of democracy, and opens up larger spaces for its spreading and amassing, even more than the Islamistic extremism itself would do it.

References:

1. *3 Brothers Sentenced to Life for Holy War Plot at Ft. Dix*, (28. 4. 2009), The New York Times, str. A19.

2. *367 ljudi bez državljanstva BiH*, (11. 4. 2007). B92 Vesti. Retrieved from http:// www.b92.net/info/vesti/index.php?yyyy=2007 _category=167&nav_ id= 24 1381.

3. Al-Alawi, I. (24. 9. 2012), *Extremists Establish Foothold in the Balkans*, Gatestone institute. Retrieved fromhttps://www.gatestoneinstitute.org/3360/ kosovo-peace-tv.

4. *Albanian terror suspects appear in Montenegro court*, (15. 5. 2007), B92 Vesti, Retrieved from https://www.b92.net/eng/comments.php?nav_id=41225.

5. Archick, K., Rollins, J, in Woehrel, S. (2005), *Islamist Extremism in Europe*, Washington DC: Congressional Research Service.

6. Ash, T. G., (2001), *Le Kosovo en valait-il la peine ?*, Le Débat, 114 (2), 53-70.

7. Atran, S., (15. 11. 2015), *Mindless Terrorists? The Truth about ISIS is much worse*, in The Guardian. Retrieved from https://www.theguardian.com/ commentisfree/2015/nov/15/terrorists-isis

8. Azinović, V., (2015), *Bosnia and Herzegovina and the Nexus with Islamist Extremism*, Democratization Policy Council.

9. Azinović, V. in Jusić M., (2016), *Novi zov rata u Siriji i bosanskohercegovački kontigent stranih boraca*, Sarajevo: Atlantska inicijativa.

10. Babanovski, I., (2002), *ONA – teroristička paravojska vo Makedonija*, Skopje: Veda.

11. Babuna, A., (2003), *Albanian national identity and Islam in the post-communist era. Balgat*, Ankara: Center for Strategic Research (SAM). Retrieved from http://sam.gov.tr/albanian-national-identity-and-islam-in-the-post-communist-era.

12. Baer, R., (2008), *The devil we know: dealing with the new Iranian superpower*, New York: Crown Publishers.

13. *Balkan u kandžama vehabija*, (29. 10. 2011), Večernje. Retrieved from http://www.novosti.rs/vesti/naslovna/hronika/aktuelno.291.html:351204-Balkan-u-kandzama-vehabija.

14. Bardos, G. N., (2005), *Containing Kosovo*, Mediterranean Quarterly, 16 (3), 17-43.

15. *Biće dana za džihada*, (14. 2. 2005), Večernje novosti. Retrieved from http://www.novosti.rs/vesti/naslovna/drustvo/aktuelno.290.html:166622-Bi263e-dana-za-dzihada.

16. *Bin Laden opens European terror base in Albania*, (29. 11. 1998), Sunday Times. Pridobljenona http://www.kosovo.net/kla_obl.html.

17. Bećirević, E., (2016), *Salafism vs. Moderne islam – A Rhetorical Fight for the Harts and Minds of Bosnian Muslims*, Sarajevo: Atlantic Initiative.

18. *Borba vlasti u BiH protiv terorizma*, (9. 4. 2008), Southeast European Times. Retrieved from https://www.vesti.rs/Vesti/Borba-vlasti-u-BiH-protiv-terorizma.html.

19. *Bosnia and Herzegovina: Attitudes on Violent Extremism and Foreign Influence*, (2017), Centre for Insights in Survey Research, International Republican Institute (IRI), January 4 - February 3. Retrieved from http://www.iri.org/sites/default/files/iri_bosnia_poll_february_2017.pdf.

20. Brisard, J. C., (2002), *Terrorism Financing*, Report for the President of the UNSC, 19.

21. Casoli, P., (29. 12. 2007), *Terror & amp; Gratitude: Albanian Imam's Kosovo Mission*. Serbianna.com. Retrieved from http://www.serbianna.com/columns/casoli/001.shtml.

22. Central Intelligence Agency [CIA], (2018), *Albania*. Retrieved from https://www.cia.gov/library/publications/the-world-factbook/geos/print_al.html

23. Çinar, B. in Gonzalez, M. E., (2013), *Democracy, Islam and Politics in Modern Albania. Süleyman Demirel University*, The Journal of Faculty of Economics and Administrative Sciences, 18(2), 119-142.

24. CSSTR, *Annual Reports: 2007*, 2011.

25. Deliso, C., (2007), *The coming Balkan caliphate: the threat of radical Islam to Europe and the West*, USA: Westport, Conn: Praeger Security International.

26. Dikici, A., (2008), *Preventing the PKK's misuse of children by introducing community policing: the Şanlıurfa case*, Defense against terrorism review, 1(2), 119-138.

27. Đurđević D. Ž., Stevanović M., Mitić V. in Kocić Lj., (2016), *Fractal tools in terrorist and financial crime prevention*, in Vojislav Mitić, Lidija Mančić in Nina Obradović (Ed.), *Advanced Ceramics and Application: new frontiers in multifunctional material science and processing,* 5th Serbian Ceramic Society Conference, Belgrade, 21-23. September (str. 55–56), Belgrade: Serbian Ceramic Society, Springer.

28. *Europe: Integrating Islam*, (2011), Council on Foreign Relations. Retrieved from https://www.cfr.org/backgrounder/europe-integrating-islam.

29. Fares, V., (2008), *Džihad u budućnosti*, Beograd: Narodna knjiga – Alfa.

30. Farnam, A., (26. 9. 2003), *Gun culture stymies the UN in Kosovo*, in The Christian Science Monitor. Retrieved from https://www.csmonitor.com/2003/0926/p08s01-woeu.html.

31. *Frankfurt airport shooting suspect Uka denies terrorist training*, (19. 1. 2012), Stars and Stripes. Retrieved from http://www.stripes.com/news/europe/frankfurt-airport-shooting-suspect-uka-denies-terrorist-training-1.166305.

32. Frieden, T., (19. 8. 2004), *FBI: Albanian mobsters 'new Mafia'*, CNN international. Retrieved from www.cnn.com/2004/LAW/08/18/albanians.mob/index.html.

33. Grizold, A., in Zupančič, R. (2008). *Analiza konflikta v Makedoniji. Teorija in praksa*, 45 (3-4), 324-344, Ljubljana: Univerza v Ljubljani.

34. Hamad, A., (2007), *U mreži zla – Međunarodni terorizam i Al Kaida,* Banja Luka: Glas Srpske.

35. Huszka, B., (2007), *The Presevo Valley of Southern Serbia alongside Kosovo: The Case for Decentralisation and Minority Protection*, CEPS Policy Brief, 120.

36. *Islamska zajednica Crne Gore ograđuje se od vehabija*, (2018), Rijaset islamske zajednice Srbije. Retrieved from http://www.rijaset.ba/index.php?option=com_content zajednica-crne –gore-ogradjuje-se-od-vehabija&catid=41 Itemid=629.

37. Jerotić, V., (2016), *Hrišćanstvo i islam*, Beograd: Ars Libri.

38. *Kako se finansiraju i naoružavaju vehabije i džihad*, (21. 4. 2012), Dan (Podgorica).

39. Kastrati, A., (8. 10. 2015), *The Relationship Between Islam and Democracy in Kosovo: The Roles and Contributions of the Religious Leaders in the Democratization Process*, in European Scientific Journal. Special edition, Vol. 1. Retrieved from https://ssrn.com/abstract=2910627.

40. Kelley, J., (26. 11. 2001), *Bin Laden's training camps teach curriculum of carnage*. USA Today, 1A.

41. Lieberman, J. I., in Collins, S., (2008), *Violent Islamist Extremism, The Internet, and the Homegrown Terrorist Threat*, Majority and Minority Staff Report. United States Senate: Committee on Homeland Security and Governmental Affairs.

42. Lobnikar, B., Prprović, B., Nemec, N., Banutai, E., Prislan, K. in Cajner Mraović, I., (2016), *Comparative analysis of the quality of policing in local Slovenian and Croatian multicultural communities,* in Revija za kriminalistiko in kriminologijo, 67(4), 275–288.

43. Mahnaimi, U., (22. 3. 1998), *Iranians Move In*, Sunday Times (London).

44. Makarenko, T., (2004), *The crime – terror continuum: tracing the interplay between transnational organised crime and terrorism*, Global crime, 6 (1), 129-145.

45. Matoshi, H., (2001), *The Albanian´s New Model Army*, IWPR´S BCR, 2(4). Retrieved from http://www.iwpr.net.

46. *Međunarodni znanstveni simpozij Islam i mediji*, (22. 4. 2015), Islamska zajednica u Bosni I Hercegovini. Retrieved from http://www.islamskazajednica.ba/index.php?option=com_contentgreb-medunarodni simpozij- islam-i-mediji&Itemid=457.

47. Mitić, V. V., Kocić, Lj. M., Tidrow, S. in Fecht, H. -J., (2017), *Structures, Fractals and Energy*, in B. Raj, M. Van de Vorde, Y. Mahajan (eds.), *Nanotechnology for Energy Sustainability*, Vol. 2, 781-808. Weinheim: Wiley-VCH Verlag GmbH&Co KgaA.

48. *Muslimani i Islamska zajednica u Crnoj Gori*, (2. 1. 2011), *Islam Montenegro*, Retrieved from http://www.monteislam.com/islamske-teme/muslimani-i-islamska-zajednica-u-crnoj-gori.

49. Mutschke R., (13. 12. 2000), *The Threat Posed by the Convergence of Organized Crime, Drugs Trafficking and Terrorism,* Statement. Hearing before Committee on the Judiciary, Subcommittee on Crime, Serial no. 148. Retrieved from http://commdocs.house.gov/committees/judiciary/hju68324.000/hju68324_0f.htm.

50. *Na putu u nemačkoj varošici utisnut natpis UÇK*, (9. 8. 2017), B92-info. Retrieved from https://www.b92.net/info/vesti/index.php?yyyy=2017id=1291467.

51. Öktem, K., (2010), New *Islamic actors after the Wahhabi intermezzo: Turkey's return to the Muslim Balkans*, European Studies Centre, University of Oxford, 2-57.

52. *Opasni bosanski tango: Islam i nacionalizam*, (2013), Evropska analiza Krizne grupe, 70.

53. Panovski, A., (2011), *The Spread of Islamic Extremism in the Republic of Macedonia*, California, Monterey: Naval Postgraduate School.

54. *Paradžemati raspostranjeni širom BiH. Ima ih 64*, (20.1.2016), Večernji list. Retrieved from https://www.vecernji.ba/vijesti/paradzemati-raspostranjeni-sirom-bih-ima-ih-64-uglavnom-su-po-brdima-1053427.

55. Precht, T., (2007), *Home grown terrorism and Islamist radicalisation in Europe*. Danish Ministry of Justice. Retrieved from www.justitsministeriet.dk/ .../2007/Home_grown_terrorism_an

56. *Predivan miris šehida u zemlji džihada*, (29. 8. 2013), Allahova-milost.blogspot.com Retrieved from http://allahova-milost.blogspot.rs/2013/08/predivan-miris-sehida-u-zemlji-dzihada.html.

57. Prifti, P. R., (1978), *Socialist Albania since 1944*, Cambridge: MA MIT Press.

58. Radeljić, B., (2010), *Growing Concerns about Islam in the European Union*, Review of International Affairs, 61(1140), 5-22.

59. Raimondo, J., (29. 10. 2001), *Osama in the Balkans*, Antiwar.com. Retrieved from https://www.antiwar.com/justin/j102901.html.

60. Rakić, M. in Jurišić, D., (2012), *Wahhabism as a Militant Form of Islam on Europe's Doorstep*, Studies in Conflict & Terrorism, 35(9), 650-663.

61. Sandić, K., (2011), *Finansiranje terorizma putem pranja novca*, Beograd:Nauka i društvo.

62. Selimi, K., in Stojkovski, F., (2016), *Assessment of Macedonia's Efforts in Countering Violent Extremism*, View from Civil Society. Skopje: Analytica.

63. Shay, S., (2008), *Islamic Terror and the Balkans*, New Brunswick:Transaction Publishers.

64. Simeunović, D., (2008), *The violence as social pathology of young people in the Balkans*, Đ. Ignjatović (prir.), *Stanje kriminaliteta u Srbiji i pravna sredstva reagovanja*. Deo 2 (pp. 125- 129). Beograd: Pravni fakultet Univerziteta.

65. Simeunović, D., (2009), *Terorizam*, Beograd: Pravni fakultet Univerziteta u Beogradu.

66. Simeunović, D., (2012), *Home-grown Terrorism as a Challenge for Homeland Security*, in J.P.I.A.G. Charvat, (ed.), *Homeland Security Organization in Defense against Terrorism*, 167-177, The Centre for Excellence – Defense against

Terrorism (COE- DAT). Advanced Research Workshop in Ankara, NATO. Amsterdam; Fairfax, VA : IOS Press.

67. Simeunović, D., (2014), *Home-grown Terrorism in United States and its Links to Balkans* ("White Al Qaida"), International Journal of Multidisciplinary Thought, pp. 497-508.

68. Simeunović, D., (2016a), *Contemporary jihadism as ideology being used by terrorist organizations*, Rocznik Bezpieczeństwa Międzynarodoweg, 10.

69. Simeunović, D., (2016b), *Islamska država (ISIL, ISIS, DAEŠ)*, Nacionalna bezbednost [National Security] 3, pp. 7-39.

70. Simeunović, D., in Dolnik, A., (2013), *Security Threats of Violent Islamist Extremism and Terrorism for South East Europe and Beyond*, in Sh. Cross, S. Kentera, R. Vukadinovic and R. Craig Nation, (Eds.), *Shaping South East Europe's Security Community for the Twenty-First Century* (pp. 87-113), London: Palgrave Macmillan.

71. Stojančević, V., (2016), *Džihad u istoriji Balkana*, Beograd: Nauka i društvo.

72. Tadić, D., (2017), *Lack of Good Governance Contributes to Growth of Radical Islam in the Western Balkans*, Clingendael Spectator, 71 (4). Retrieved from https://spectator.clingendael.org/pub/2017/4/the-growth-of-radical-islam/

73. Taneski, N., (2010), *Radikalniot Islam: Realna zakona za bezbednost na Balkanot. Društvena reakcija na savremene oblike ugrožavanja bezbjednosti*, Banja Luka: Fakultet za bezbjednost i zaštitu.

74. *Terorizam i Srbija - džihadisti među nama*, (18. 11. 2014), Svetinje Braničeva. Retrieved from http://svetinjebraniceva.rs/index.php?option=com_content 18-06-58-11&catid=38:2010-12-14-18-00-48&Itemid=59, 18. 11. 2015.

75. *Teroristi u institucijama BiH*, (20. 1. 2015), B92-info. Retrieved from https://www.b92.net/info/komentari.php?nav_id=948758.

76. Thachuk, K. L., Bowman, M. E. in Richardson, C., (2008), *Homegrown terrorism: The threat within*, Washington DC: National Defence University, Center for Technology and National Security Policy.

77. *The Prevent–Refer–Address Mechanism* (P-R-A), (24. 7. 2017), WBCTi. http://wbcti.wb-iisg.com/blog/2017/07/24/prevent-refer-address-mechanism-p-r-a.

78. *The unexplored nexus: issues of radicalisation and violent extremism in Macedonia* (2018), Report by KCSS (Kosovar Centre for Security Studies), 03.

79. *The Western Balkan Counter-Terrorism initiative* (2018), IISG. Retrieved from http://wb-iisg.com/docs.

80. Tok, E., Calleja, R. El-Ghaish, H., (2014), *Arab development aid and the new dynamics of multilateralism: Towards better governance*? European Scientific Journal, Vol. 1, pp. 591-604.

81. *Trading Economist*, (2018), *Albania Unemployment Rate 1993-2018*. Retrieved from https://tradingeconomics.com/albania/unemployment-rate.

82. Trading Economist, (2018a), *Bosnia and Herzegovina Unemployment Rate 2007-2018*. Retrieved https://tradingeconomics.com/bosnia-and-herzegovina/unemployment-rate.

83. Trading Economist, (2018b), *Kosovo Unemployment Rate 2001-2018*. Retrieved from https://tradingeconomics.com/kosovo/unemployment-rate.

84. Trading Economist, (2018c), *Montenegro Unemployment Rate 2002-2018,* https://tradingeconomics.com/montenegro/unemployment-rate.

85. Trading Economist, (2018d), *Serbia Unemployment Rate 2008-2018*, Retrieved from: https://tradingeconomics.com/serbia/unemployment-rate.

86. *Trading in Misery*, (5. 9. 2003), IWPR Balkan Crisis Report.

87. *Trieste Western Balkans Summit: Declaration with recommendations stemming from the Civil Society Forum*, including the RECOM initiative (12. 7. 2017), RECOM. Retrieved from http://recom.link/trieste-western-balkans-summit-declaration-recommendations-stemming-civil-society-forum-including-recom-initiative.

88. *US hunt Islamic militants in Bosnia*, (26. 7. 2004), The Daily Telegraph (UK). Pridobljenona http://www.slobodan-milosevic.org/news/dt072604.html

89. *Uskoro će vas velika tragedija pogoditi, zora islama je stigla, ISIS se vraća na Balkan i preti. Usamljeni vukovi spremaju pokolj za praznike*! (5. 12. 2017), Telegraf. Retrieved from http://www.telegraf.rs/vesti/jugosfera/2917157.

90. Vidino, L., (2006), *Al Qaeda in Europe: The New Battleground of International Jihad*, Amherst, New York: Prometheus Books.

91. *Vulnerability and Resilience to Violent Extremism in selected communities in Bosnia and Herzegovina, the Former Yugoslav Republic of Macedonia, and Kosovo*, (2017), Preliminary Regional Inception Assessment Report. International Organization for Migrations [IOM].

92. *Wahhabis sang song for Bin Laden*, (17. 8. 2010), Utrinski vesnik. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a556492.pdf.

93. Wilkinson P., (2002), *Terorizam protiv demokracije*, Zagreb: Golden marketing.

94. Woehrel, S., (26. 7. 2005), *Islamic Terrorism and the Balkans,* CRS Report for Congress. Washington DC: Congressional Research Service: The Library of Congress.

SECURITY AND THE FIGHT AGAINST TERRORISM AS KEYS TO REGIONAL STABILITY: ROMANIAN LESSONS

Lt. gl. (r) Florian COLDEA*

Abstract

The paper aims at analyzing, from a practitioner's perspective, security problems and patterns for South Eastern Europe, ranging from terrorism to Russian influences, as well as potential common solutions for them. It will review the variety of reasons for which this particular region is considered of great importance and interest from a strategic point of view, such as being an "unquiet frontier", a weak zone or "soft spot", and why the subject should be very high on the agenda of policy-makers, security analysts and practitioners alike, academics and various other institutions.

I intent to case-study Romania`s manner of dealing with security risks, which I consider significantly superior to those of some of its neighbours', the success of its historical and current security strategies, and the lessons which our country can provide for the region. In my opinion, the key for all SEE member states to achieve a safer status is capacity building. And capacity building cannot be obtained by individual efforts of the Eastern European countries alone, but rather through a solid system of support, encouragement, and help from regional and Western partners and allies. Current cooperation formats as well as potential ones, including NATO and EU enlargements, will also be reviewed, since they constitute the main security solutions for unstable and insecure countries in the region.

Keywords: *#unquiet frontier, #terrorism, #Russian influence, #cooperation, #capacity building.*

Overview of the Region

Due to a variety of reasons, South Eastern Europe is considered an area of great importance and worthy of significant interest from the strategic point of view: it has a particular geography and unique history, radically different from that of Western European states, constituting both a physical

* Associate Professor, "Mihai Viteazul" National Intelligence Academy, coflorian2017@gmail.com.

extremity for the European continent and a fringe for traditional alliances such as NATO and EU. With all advantages stemming from its geographic location, it is also what Wess Mitchell and Jakub Grygiel have called an *unquiet frontier (*Grygiel and Mitchell, 2018*)*, a weak zone or soft spot, prone to intrusions of various natures, which need to be addressed as such, advantages and disadvantages included.

Part of the interest for this region stems from its status as contact point for Western values and alliances with one of the foremost challengers to the status of global power[1] of our time, the Russian Federation. This border status makes the region particularly vulnerable, even more so since its strong, prominent allies are at the weakest at the margins of their influence; this makes regional actors more prone to shifting sides when pressed, if not enough support comes from traditional allies. The potential for regional conflict is still high in an area which has sparked both World Wars, and the Cold War.

Concerning common historical traits, during the Cold War, most countries in the region were part of the Warsaw Treaty, had communist regimes, therefore had little or no contact with democratic values, no freedom of speech, and the concept of free media was unknown to them[2]. Economy in former USSR satellites was centralized, obviously dysfunctional, most times corruption-generating, as well as lacking notions such as private property. Those characteristics are also reflected, in different degrees, in today`s economical underdevelopment of the region, and in the pervasive corruption, and both factors are only aggravating for most security threats.

During the Cold War, countries in the region used to have extensive military capabilities and large armies, but not professional ones, while intelligence services were strong and effective with regards to countering terrorism, but also reputable weapons in maintaining the political *status quo*. From the security point of view, basically, during the Cold War and

[1] Wess Mitchell and Jakyub Grygiel actually call Russia a revisionist power, aiming at becoming as influential as it was at the apex of its power. According to the same authors, revisionist states try to challenge not necessarily the global order, but rather the regional one, by trying to reap benefits – including annexation of territories they had previously controlled –from political control over neighboring states; although their ambitions are regional, their effects have the potential of creating worldwide instability. See Grygiel and Mitchell, p. XXV.

[2] Surprisingly, from the national security standpoint, controlled media turned out to be somewhat an advantage, because state-controlled press made no references to terrorist attempts or attacks, therefore the propaganda purposes of terrorist organizations could not be fulfilled.

afterwards, the SEE countries had a low terrorist threat, and relatively few terrorist incidents.

It is important to mention that most of the former Soviet satellite-states had no problem with religious minorities (except for the former Yugoslavia), and, as to religiously-motivated terrorism, they only had small and old domestic Muslim communities, well integrated and moderate. Most countries in the region – Romania among the most prominent – also had good diplomatic, cultural, and economic relations with Muslim states, while communist leaders had close personal ties with Arab and Muslim ones, which helped them and their countries stay safe. A notable exception from this general trend is, of course, Turkey, which has a generally moderate Muslim population, but is known for being "a top notch area where (terrorist) operations targeting the European continent are organized, and where they (terrorists) withdraw" (Migaux, 2018).

The Autumn of Nations and the subsequent second wave of revolutions at the beginning of the '90s brought about political and economical instability, and power vacuum; the fall of the USSR and dismemberment of the Warsaw Treaty left former satellite states leaderless, disoriented, and in a difficult and prolonged transition. Economically, their situation was difficult, while from the point of view of security, it was a *grey area*, with several actors struggling to gain influence: Russia, the US, and the EU. Democratic values were inexistent or at a minimum, and acquiring such values was a long, painstaking process, in some instances still ongoing as we speak.

While the period before 2001 was marked by global stability – let`s not forget about Fukuyama`s proclaimed *end of history* –, for SEE, it was marred by regional instability. Frontiers were reorganized, and serious military conflicts took place. However, with regard to the terrorist threat, extremist nationalist attacks tended to be less frequent, while religious minority problems increased only slightly, overall. There was only a slow growth of the Muslim community, which was, however, still well integrated and with a low level of radicalization. Countries in the region still enjoyed overall good relations with Muslim countries, mainly by virtue of their former ties. Low levels of the terrorist threat and relatively few terrorist incidents were still a major advantage of the region. Security and stability were achieved to a higher degree by most states only once they became NATO members.

SEE states` accession to NATO had the major advantage of mitigating potential sources of conflict in the region, dissuading Russian military interventions, and suppressing regional territorial disputes. It is relevant for countries in the former Soviet sphere of influence that they sought security first and foremost. Political and economic alliances came second to the

necessity of NATO integration. Accession was, in some cases, a three step process, consisting of Partnership for Peace Membership, Membership Action Plans, and, eventually, full integration.

NATO accession meant operating difficult but effective reforms of the security sector: national armies were professionalized; defence infrastructure was modernized, while intelligence services were reformed in order to overcome political police suspicions. The intelligence organizations from the communist period were dissolved, and they handed over their archives, most of which were made accessible to the general public. New intelligence agencies took over, with some of the old inheritance, but making radical changes in personnel, regulations and preoccupations, while also being held to new democratic and professional standards, which were further validated by Euro-Atlantic allies and partners.

For Romania, making the shift from an authoritarian regime to a democracy, passing through a long and painstaking transition, was anything but simple, but it was mandatory. Based on Romania's experience, as well as those of other countries in the region, sooner rather than later, people do support this difficult process towards democracy, choosing to be part of the solution, and not the problem, even if they are under different pressures, like hybrid war, assertiveness of revisionist powers, radical Islamic influence, terrorism, migration, separatism, Chinese persuasions etc.

Despite all progress and despite its relative safety from the terrorist threat, currently, SEE is still a weak point for the European continent: it exports instability, due to its ethnic conflicts and territorial rivalries, as well as organized crime, connected to trafficking human beings, weapons or drugs, or even cybercrime, which has found a safe haven in some countries. Those complex vulnerabilities need to be tackled and solved as soon as possible, since they are exploited by all kinds of interested parties, from Russia, which uses and deepens them in order to gain influence and economic advantages, to China, which invests heavily in the region and tends to spy as heavily, or to some Muslim countries which try to fund and support radical Islamic communities in the area.

As for the current regional status, at least two particular events can significantly alter the status of the region; first of all, the negotiations for swapping territory among Kosovo and Serbia, aiming at making them both more ethnically homogenous. Various factors, like Serbia`s tight relations to Russia, or the EU`s divided attitude towards such arrangement, already rejected by chancellor Angela Merkel, make it a questionable deal. The second essential event for the region`s stability is the referendum in Macedonia over the name dispute (*Why Efforts to Build Bridges Could Threaten Peace in the*

Western Balkans, 2018), which could effectively end a serious source of tensions with Greece, but is rather shaky since nationalist have already caused violent protests against the deal, the Macedonian president himself is boycotting the deals, and the two parties in the ruling coalition have opposite views on the Macedonian affair. Good results in these matters would lead to a betterment of the regional stability, better relations between neighbouring countries, and EU accession for some of the involved parties, with all economic and political consequences.

Terrorism in South-Eastern Europe

With regard to terrorism, particularly the religiously motivated one, countries with old, moderate Muslim communities have a competitive edge, since they are prone to support the integration of potential newcomers. This is highly relevant in the context of the immigration waves that hit Europe in the past years.

Nonetheless, currently, extremist groups are an increasingly worrisome phenomenon in the region; foreign ultra-conservatives, prone to radicalization and generating tensions in the receiving societies, managed to cause some religious communities to reject local religious authorities, and even state authorities. Social values widely accepted in SEE societies tend to be contested by radical Islamist newcomers, which provokes a further widening of the gap between European societies.

The region has built the necessary counter-terrorist capabilities, which are in place at levels similar to those of our Western partners and allies, but – fortunately – were never fully tested. And although the threat level is considered low in the area, states such as Romania and Bulgaria are entry points for terrorist militants targeting the West. The countries` involvement in peace-keeping missions in the Middle East also led to an increase of terrorist risks. There were also allegations regarding readily accessible nuclear material in former communist countries, which could easily have become ammunition for terrorist operations.

The most relevant and worrisome facet of the terrorist phenomenon in SEE is that of foreign fighters and returnees. Several Eastern European countries are placed on the main routes used by European foreign fighters in order to travel to areas of conflict (mainly to Syria and Iraq). Moreover, there are states in the Western Balkans with a sizable Muslim population out of which more than 1,000 people have travelled to conflict areas (Petrovic, 2019), the most prominent being Kosovo, and Bosnia Herzegovina. Worth noticing the fact that these jihadists are mostly young males (between 20 and

35 years of age), coming from remote rural areas, usually poor, unemployed and lacking work experience or skills (Beslin and Ignjatijevic, June 2017). This brings up the important questions of how much of this process is generated by ideology, and how much is financial gain involved in motivating those youngsters to join violent fights. Gl. Kircio Kirov, former chief of Bulgarian NRS, publicly stated, in 2017, that there are premises for activation of sleeping terrorist cells, with the return of DAESH foreign fighters in Albania, Kosovo, FYROM, Montenegro, and Bulgaria.

Radicalization and home-grown terrorism are also becoming increasingly relevant for the region`s security environment. Romania, for example, does not have an extensive radicalization issue as yet, nor home-grown terrorism to such an extent as to be called a phenomenon, but there have been isolated cases in which young people engaged or planned to engage themselves in radical activities. There is a growing need to pay attention to the isolated cases of Romanian converts, who are more prone to adhere to the extremist interpretations of the Islam.

Other states in the area were, nonetheless, more affected by the radicalization and recruitment process. The local, moderate Muslim community, also secularized by prolonged communism, was infused with radical Muslims in the 1990s, when an estimate of 2000 Arab Mujahedeen fighters came to the aid of Bosnian Muslims, in the Yugoslavian wars. Some of them settled in the region, and contributed to the radicalization process, particularly in rural, poor areas, with high unemployment and a precarious economical state. Funds from the Middle East supported mosques, radical Islamist canters offering what seemed like social services to communities, and NGOs, which degraded the regional security environment.

Later on, particularly in the Balkan-Slavic regions, Al-Qaeda was thought to have developed extensive recruitment campaigns in 2003-2004, aiming at Slavic Muslim from Bosnia, Albania, and Kosovo. For a period after the 9/11 shock, the Balkans were thought to be a new general headquarter for Islamic terrorism operations targeted at Western Europe. Strong Al Qaeda cells were established in Albania, Kosovo, and Macedonia in the first five years after 9/11. Porous borders and endemic corruption were considered the main reasons allowing for those negative developments.

A special note is to be made on the extent and the very significant role of the current online activities in radicalization, indoctrination and communications among people interested in the Jihadist ideology. In an era marked by limitless communication, the shadow of anonymity offered by chat-rooms and forums or by the Dark Web enables jihadist to indoctrinate and recruit vulnerable youngsters, to support and fight for terrorist organizations.

Most countries in the region managed to update their legislation, in order to prevent and punish terrorist funding, as well as recruitment (on-line included) and fighting abroad. A Pew Research Centre study as of 2017 showed that most Muslim communities in the Balkan countries have an overall reduced support for conservative Islam. The Sharia Law had percentages of support among the Muslim population of maximum 20% in Kosovo – which is actually something to worry about, in my opinion, and 12% in Albania (Lipka, 2017).

As expected, migration also has a direct impact in increasing terrorist risks and is currently difficult to assess. Migrants can be terrorists and terrorists can be migrants. Balkan states are not as affected by the phenomenon as other Southern European countries, but it is important to note that rising anti-immigrant sentiments, even in countries which are not destination, nor transit countries, is distancing SE European partners from their Western counterparts.

Romania is a positive example in countering terrorism. Romanian intelligence services entered the "first league" of counter-terrorist fighters in 1995, when they caught an important Japanese Army member, responsible for several bombings on public Japanese targets. We managed to avoid any attack on our national territory, although, as I described it above, the regional context wasn`t entirely peaceful, nor was it really secure. Romania understood, in the aftermath of the 9/11 attacks, that it needed a prompt reaction in order to prevent such events and this understanding generated first of all legal and administrative reforms which would allow, for a while, for proper counter-terrorist prevention. Authorities acted concerted and proactively, passing relevant legislation regarding terrorist financing, but also supporting intelligence gathering and close cooperation among many state institutions and authorities with relevant roles in the matter. The Romanian National System for Preventing and Countering Terrorism (SNPCT) was the first structure of its kind in Eastern Europe, and it instituted a flexible cooperation mechanism, as well as capabilities for swift crisis reaction. It succeeded in cutting funds for some terrorist cells (Coldea, 2017, pp. 111-116) and became a role-model for other states in the region.

Prevention became the main preoccupation for Romanian intelligence with respect to terrorism, which actually helps project security in neighbouring countries, as well.

Russian influence

Different, but just as significant factors in regional stability are outside influences, some helping the security climate, others undermining it. As mentioned in the introduction, there is a tendency of some revisionist states – among which Russia, China, and Iran – to try and change the global balance of power, and to challenge the hegemony of the United States. And what better way to do this if not by trying to attract the allegiance of border states – such as those in SEE, trying to include them in a new sphere of influence, in order to achieve various domestic goals?

Russian lack of access and influence in the region means it is deprived of instruments for making a clear statement in the European balance of powers. It has no gateway to central Europe, due to Poland`s resistance, not enough control over energy routes, no access to the Mediterranean Sea, due to Romanian and Bulgarian opposition. Deprived of influence, Russia is, thus, only another Eurasian powerful state.

Regional attitudes towards Russia vary between two poles: the "balancers", such as the Baltic States and Romania, keep a consistent resistance strategy, while some of the region tends to maintain closer ties with the Eastern neighbour, placing economic interests above political objectives. Bulgaria, for example, although a NATO and EU member, kept a particularly tight relation to Russia, choosing, among others, to enter the South Stream project, and ignoring EU anti-trust regulations.

Russia is also ubiquitous in Serbia. This is not entirely surprising, since Serbia is enjoying a status of military neutrality and is currently remaining out of the EU, although a candidate for membership. When Russia continues to provide support for a strategically ambiguous Serbia, it also suggests that Serbia's full membership of the EU may not be compatible with the principles of the Free Trade Agreement that Serbia has signed with the Eurasian Economic Union.

That said, a geopolitical convergence reinforced by the links of the Orthodox religion, which are still central to Russian foreign policy, appears to reach its limits, as we can currently observe in the Balkan region.

As for the EU, there are six states included in the EU's Eastern Partnership: Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine, all with different national specificities, democratic tradition (or lack of), and long-term interests. Russia takes advantage of the EU`s indecision to fully politically support the Eastern Partnership countries, and employs a wide – and mostly already known – array of tactics to keep these states under its sphere of influence and control.

A secondary reaction to the resurge of Russian interest in generating a new sphere of influence, difficult to anticipate in the `90s, was a tendency of the neighbouring countries to make new provisions for self-defence. After having considered NATO as a security warranty for some time, states in the region started to increase defence spending and enhance their defensive capabilities. In this regard, Latvia, a country prone to invasions similar to the Ukraine one, due to its large Russian community, increased defence spending by 12%. Lithuania increased spending by 40% in 2014, anticipating further increases.

Romania also increased defence spending by 15% in 2014, due to the Ukrainian crisis, and to potential Russian threats to neighbouring Moldova, and, by 2017, it even fulfilled the NATO target of allocating 2% of GDP for defence, alongside Estonia, and just under Greece spending. Bulgaria has also constantly increased budgetary allocations for defence.

Military analysts also noticed a tendency of SEE states to return to traditional means of defence, renouncing pretensions of interoperability with the US, or forces necessary for joint interventions. The Estonian concept of security, for example, was focused on international peacekeeping missions at the beginning of the Millennium, while in 2011; it rather reverted to conventional threats, considering the possibility that small states could, at a difficult crossroad, lack necessary support from the international community.

Russian influences are, however, difficult to counter in the region; we were, obviously, not ready for this type of hybrid war, which includes fake news, manipulation and propaganda, able to easily persuade a rather poor, uneducated population, as it is the case in South Eastern Europe. A European Political Strategy Centre analysis as of May 17th 2018 (*Engaging with the Western Balkans,* 2018) reveals that lack of criticism towards fake narratives is much higher in the Balkans than in EU-member states, quoting resilience to harmful narratives to an index of 56 in the EU, 31 in Serbia, and a minimum of 10 in FYROM.

Cooperation is the Key

We are only as strong as our weakest link; therefore, as neighbours and allies in the region, we need to help each other in order to make this area a more secure one. Aggregating capabilities and resources makes for a more effective security strategy, consequently cooperation is tantamount to security. Cooperation is already well established on two levels: strategic orientation, stemming from alliances and partnerships such as EU and NATO,

as well as operational orientation, dedicated to intelligence, military, and security policies.

The EU has multiple initiatives dedicated to the issues at stake as the Eastern neighbourhood represents a strategic position with important connections to Central Asia, the Middle East, but also to the Western Balkans, with a great potential to develop energy, transport and commercial routes, and a high relevance of issues like environment or democracy.

The EU approach towards the countries that form its Eastern frontier is to support their stability, predictability and European path – based on instruments related to the *European Neighbourhood Policy* and, implicitly, the *Eastern Partnership.* The main priorities of the ENP (as of November 2015) concern: building resilience to the new threats, reforming the security sector, border protection, judicial cooperation and combating terrorism and radicalization, corruption and organized crime. But, by virtue of the new "differentiation principle", each partner state can decide on the speed and depth of the partnership and the domains it covers.

With regards to law enforcement cooperation on pertinent matters for regional security, the EU`s EUROPOL dedicates resources to countering international terrorism, as well as organized crime, supporting law enforcement in all member states. Intelligence cooperation is, nonetheless, not in the EU`s purview, since national security is, according to the EU Treaty, a matter of exclusive domestic concern.

The EU is also, by far, the largest investor in the SEE, accounting for over 75% of all direct foreign investments in the region in the 2007-2016 timeframe (*Engaging with the Western Balkans, 2018*).

Table 1: The EU remains by far the largest investor in the Western Balkans
Foreign Direct Investment inflows, in million euros, 2007-2016
(*Source*: Vienna Institute for International Economic Studies, FDI)

EU28	China	Russia	Saudi Arabia	Turkey
21,031	2,727	1,126	233.2	110.6

Nevertheless, this hasn`t necessarily increased the EU`s popularity in the region, with population and leaders caught between Russia`s struggle for influence, and temporary personal and political interests. A Balkan Barometer by the same Vienna Institute for International Economic Studies (*Engaging with the Western Balkans, 2018*) shows that, since political elites in some of the SEE countries have frequently sought to use all advantages the EU had to

offer to their own interests, people saw little or no real progress, and they were disappointed with the European solution. While EU favourability was rather high in the 2007-2016 timeframe in Kosovo, exceeding 90%, it reached a minimum in Serbia, of just under 30%, with averages of around 50% in Macedonia and Montenegro, and lower support in Bosnia Herzegovina, of only 32%.

As for cooperation within NATO, the Alliance proved to be aware of all regional security dangers and took some steps to respond accordingly. Especially after the illegal annexation of Crimea by Russia and in the context of Russian aggressive actions in Eastern Ukraine, we – as allies – definitely needed to establish a new approach of our relation with Moscow, and new measures to adapt and strengthen our collective defence capabilities. NATO also needs an enhanced forward presence in the East (as defence ministers already agreed in February of this year): a multinational and rotational presence that sends a clear message that crossing NATO's borders is not an option, whether it's with tanks or with 'Little Green Men', and that such action can and will be countered. The VJTF-*Very High Readiness Joint Task Force* and 6 NFIUs-*NATO Force Integration Units* (in Romania, Bulgaria, Estonia, Latvia, Lithuania, and Poland) will be the main instruments of that reassuring allied presence. The basing of the AEGIS Ashore missile defense system in Romania also contributes to overall regional security and stability. Targeting the stringent matters of terrorism and espionage, NATO has a *Civilian Intelligence Committee* (CIC), in which all member states are represented.

A significant regional defence initiative is the Northern Baltic Eight informal military alliance, which includes Lithuania, Latvia, and Estonia, alongside Denmark, Finland, Norway, Sweden and Iceland, and engages in periodical consultations, military interchange, and common exercises, while also repositioning air defence equipment, accelerating common military purchases, and increasing military spending.

Regarding intelligence and law enforcement cooperation, there are several cooperation formats that tackle directly the threats at European and regional level:

MEC – the Central European Conference includes 31 foreign and domestic intelligence services, including the ones in Balkan countries. Its objectives are to support mutual trust, reforms, and the sharing of best practices.

SEEIC – South Eastern Europe Intelligence Conference, established in 2002, for which Romanian intelligence services are among the founding members.

CTG – the Counter Terrorism Group, formed in 2004 at the EU`s request, after the New York and Madrid terrorist attacks; all member states plus Norway and Switzerland are in CTG, and it acts as an interface between the EU and member states` intelligence community.

Romania also had a particularly relevant security initiative at regional level, establishing the Bucharest-located Southeast European Cooperative Initiative (SECI), with 13 member states among which Albania, Bosnia Herzegovina, Bulgaria, Croatia, Greece, Macedonia, Moldova, Montenegro, Serbia, Slovenia, Turkey and Hungary. The organization started working in 2000 and has eight different working groups, among which a counter terrorist one.

Conclusions

Capacity building is the key for a sustainable security environment. This cannot be obtained just by the efforts of the Eastern Europe countries, but they have to be supported, encouraged and helped by Western partners, through a continuous process of "mentoring" and sharing expertise and best practices. We also need a comprehensive, coherent, and consistent legal framework which will allow all authorities to act in a swift, concerted, and timely manner in order to prevent and counter the terrorist threats.

In my opinion, durable stability in the region can be achieved by taking into account some basic principles, followed by adequate measures. First of all, policy-makers need to use the best of their possibilities at the bilateral and multilateral fora, mainly EU and NATO, in a coherent manner, to support the countries of the regions with reforms (in depth) in the fields of political, economic, social, military, law enforcement and security, education. In fact, policy-makers have to manage not only to create relevant programs (some, already in place), but to follow their actual implementation and necessary adjustments, and eventually to correctly assess the results, the impact of those programs.

Cooperation for security purposes is already well established on two levels: strategic orientation, stemming from alliances and partnerships such as EU and NATO, as well as operational orientation, dedicated also to intelligence, military, and security policies.

Further measures have to be taken by the Euro-Atlantic intelligence and law enforcement communities, to support and encourage a real reform of their counterparts in the region, and to engage them in different cooperation formats (and I am able to confirm relevant steps were made in this direction).

NATO and EU accession are viable solutions to regional peace and stability. I have personally witnessed the progresses Romania has made since its accession to NATO and the EU, as well as the difficulties and uncertainties that some of our neighbours have faced outside those alliances. Being connected to the West has always represented, sometimes in a more subtle way, an incentive and a hope for Romania. It allowed us to be proactive, to take on thorny issues, to commit ourselves to protecting national security and promoting Romania's interests. In this line of thought, even if there will never be an EU with over thirty members, I strongly believe it is of paramount importance that the Western countries continue to support the Eastern European countries, as a reassurance, even if, at times, back-steps are inevitable from both parts.

The European Union and North Atlantic Treaty Organization have done a lot for the regional security and stability, and they have created a framework towards a better context in the area: NATO gives member states the necessary impulse to consolidate their defence, security, and law enforcement, while the EU brings economic prosperity, together with rule of law, human rights, and democracy. Accession to those two organizations was a good solution for Romania, and is a good solution for the region in its entirety, the only solution which can keep it from exporting instability, organized crime, and even radical extremism. But nonetheless, much more is needed than formal adherence to those organizations: they come with adequate rules and regulations, which must be implemented, and their actual implementation must be monitored in the field. Much more needs to be done in consolidating the rule of law, as well as local law enforcement and intelligence, and NATO and EU involvement are tantamount in order to stabilize and secure SEE.

References:

1. Beslin, Jelena, Ignjatijevic, Marija, (June, 2017), *Balkan foreign fighters: from Syria to Ukraine*, European Union Institute for Security Studies (EUISS).

2. Coldea, Floria, (2017), "The Role of Authorities and Intelligence Services in the War on Terrorist Financing", in Lesenciuc, A. (ed.), *Redefining Community in Intercultural Context*. *Intercultural Pedagogy and Migration,* "Henri Coandă" Air Force Academy Publishing House, Brașov, 2017, pp. 111-116.

3. *Engaging with the Western Balkans. An Investment in Europe`s Security*, European Political Strategy Centre, May 17th, 2018, available at https://ec.europa.eu/epsc/sites/epsc/files/epsc_-_brief_-_engaging_with_western_balkans.pdf, accesed September 24th, 2018.

4. Grygiel, Jakub, Mitchell, Wess, (2018), *Frontiera neliniștită. Rivali emergenți, aliați vulnerabili și criza puterii americane,* Comunicare.ro Publishing House, Bucharest.

5. Lipka, Michael, (2017), *Muslims and Islam: Key Findings in the US and around the world,* at http://www.pewresearch.org/fact-tank/2017/08/09/muslims-and-islam-key-findings-in-the-u-s-and-around-the-world/, accessed September 11th, 2018.

6. Migaux, Philippe, (2018), "Panorama situației din 2004 încoace", in Gerard Chaliand, Arnaud Blin, coordinators, *Istoria terorismului. Din Antichitate până la Daesh*, Polirom Publishing House, Iași, 2018, p. 413.

7. Petrovic, Pedrag, (2019), *Islamic Radicalism in the Balkans,* available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/dsee/dv/10_balkan_radicalism/10_balkan_radicalismen.pdf, accessed September 3rd, 2018.

8. *Why Efforts to Build Bridges Could Threaten Peace in the Western Balkans*, Stratfor`s analysis, available at https://worldview.stratfor.com/article/why-efforts-build-bridges-could-threaten-peace-western-balkans, accessed September 9th, 2018.

THE REVIVAL OF THE INTERMARIUM GEOPOLITICAL PROJECT – THE THREE SEAS INITIATIVE AND BUCHAREST 9 FORMAT –

Vasile CREȚU*
Dragoș ARDELEANU*

Motto: *The strong do what they can while the weak suffer what they must.*
Thucydides, *The Peloponnesian War*, 1966, V. 89, p. 512

Abstract

In the light of recent crises, EU and NATO seem to be in the middle of an internal struggle to maintain their unity and cohesion. In order to create a common and stronger voice within these two structures, the Central-Eastern European countries developed two cooperation frameworks: the Three Seas Initiative (TSI) and Bucharest 9 (B9). In our vision, both emerging formats contribute to the creation of a (new) strategic North-South Axis, from the Baltic to the Black Sea, with Poland and Romania as the pillars. This is not a new concern, having its roots in the Intermarium idea, coined by Jozef Pilsudski, Marshal and leader of interwar Poland. After the First World War, he envisioned the organization of the region as a federation of states, and then as an alliance, with the purpose of countering the then-German and Russian powers. Today, we assist at the revival of the project, especially politically in Poland, but also in academic circles. The fact that the U.S. supports both initiatives gives a new impetus to the security of the region. Therefore, the aim of this paper is twofold: (1) to present the Intermarium geopolitical project and its contemporary revival through TSI and B9; and (2) to analyze the revival from a Romanian perspective, as well as to assess the implications for our country.

Keywords: *Intermarium, geopolitics, security, NATO, EU.*

* MA student, National University of Political Studies and Public Administration, v.vasilecretu@gmail.com.
* PhD, University Lecturer, "Mihai Viteazul" National Intelligence Academy, dragosardel0@gmail.com.

Introduction

Ancient Greek historian Thucydides' words are not only the motto of this paper, but also, in our opinion, a leitmotif of international relations, because power, in its different forms, is the most important factor that determines the course of events. History is full of such examples. Due to the current issue, focused on the evolutions in Central-Eastern Europe, the first example is from the regions' own history. The majority of the states from this part of Europe gained their independence in the aftermath of the First World War, on the ashes of multinational empires. On the historical scale, the existence of these nation-states is relatively new, while their populations (nations) have a much longer history. But because they were 'weak', they were the subject of foreign rule, in accordance with Thucydides' dictum.

After the First World War, a geopolitical project meant to transform Poland into the leader of Central and Eastern Europe was developed. This is the case of *Miedzymorze*, more popular in its Latin version – *Intermarium*, which means, mot-a-mot, "*between the seas*" and which originally referred to a federation or an alliance of the states between the Baltic and Black Seas. It failed to be implemented in the interwar period, being forgotten during the Cold War. Nowadays we are witnessing a revival of the project, especially politically in Poland, but also in academic circles.

Geopolitics and geopolitical ideas

Since this paper is not about geopolitics, but one of geopolitics (more specifically about a geopolitical project), only a short definition is needed, in order to underlie the theoretical framework. Defining "geopolitics" is a daunting task, especially when we acknowledge the fact that it is an over-used term in discussions about the relations between states, or the evolution of certain events. (Sempa, 2002, p. 3) Concisely, geopolitics studies the impact of geographic factors upon political decisions (Serebrian, 2003, p. 25). The basis is the understanding of geography, as Nicholas Spykman observed: "*geography is the most important factor in interstate relations because it is the most permanent. Ministers come and go, even dictators die, but mountains ranges stand unperturbed*."(Quoted in Kaplan, 2014, p. 68) Hence, the geography is the "*backdrop to human history itself*" (Kaplan, 2014, p. 66), the stage where state clashed (Sempa, 2002, p. 5), and the main motivation for it, as the territorial imperative influenced the behaviour of states over time. (Brzezinski, 2000, p. 49) Thus, geopolitics tries to explain, through its analytic methods and instruments, why an actor is interested in a region and why not in another. (Hlihor, 2005, p. 16)

Alike Robert Kaplan, who asks himself whether history is only the result of the vast impersonal forces – geographic, cultural, economic and technological – or it is influenced by extraordinary people who succeeded to overcome these forces (Kaplan, 2010, p. 204), we ask ourselves: is the impersonal force of geography the only element relevant to geopolitics? The answer tends to be negative as one looks at the global events. Through their actions, states try to turn geography into an advantage, because otherwise it remains only destiny. (Kaplan, August 14, 2014) In reality, this means following a certain path in foreign policy over the long term, on the background shaped by geography. From the theoretical point of view, the strategic thinking/culture of a nation gives birth to some conceptions – as geopolitical theories, doctrines or projects – which we will generically name 'geopolitical ideas'. Thereby, a corollary to the classic definition of geopolitics is the following: geopolitics studies not only the impersonal forces of geography, but also the ideas, which are meant to determine one state's vision about its place in the world or in one particular region.

The virtual space of these ideas covers every corner of the world. Some of them enjoy a large popularity among scholars; such is the case of Heartland and Rimland.[1] Or we could speak about pan-ideas, like Pan-Americanism, Pan-Slavism or the idea of Mitteleuropa, Eurasianism or even the subject of this paper, *Intermarium*.

Even though these ideas were developed in different eras, their applicability and relevance are still present in the 21st century, due to at least two characteristics: their connection with geopolitical reality and their flexibility. The first feature refers to the fact that every idea is well rooted in the geopolitics of that certain area (in its advantages and disadvantages). In terms of flexibility, the situation gets more complicated. This feature assumes that every idea has a margin of action, so that the adaptation is always possible, according to the geopolitical context. The basis for flexibility is the difference between the geographic and geopolitical position. While the former is unchanged as time goes by, the latter rests on global shifts or on global/regional balance of power.[2]

---

[1] A list of works dedicated to *Heartland* and *Rimland*: Keans, Gerry. *Geopolitics and Empire: The Legacy of Halford Mackinder*, 2009: Oxford University Press, New York; Petersen, Alexandros. *The World Island. Eurasian Geopolitics and the Fate of the West*. Praeger Security International, 2011; Gerace, Michael P.(1991) *'Between Mackinder and Spykman: Geopolitics, containment, and after'*, Comparative Strategy, 10: 4, 347-364; Blouet, Brian W (ed.) *Global Geostrategy: Mackinder and the defence of the West*, Frank Cass, 2005.

[2] For example, the geographical position of Romania is the same since WW2, in Central Eastern-Europe. In terms of geopolitics, we were in the "East" in the Cold War era, whilst now we are in the West, due to the NATO & EU membership.

Continual adaptation of geopolitical ideas implies assuming of the main driving principles that underlie that vision, and not every detail, which reduces from its relevance. In the case of the *Intermarium* geopolitical project, the discussion about its revival is only possible if we agree on the idea of flexibility.

The origins of the *Intermarium* geopolitical project

Every geopolitical idea is like a coin, with two sides: one theoretical, and one practical. *Intermarium* refers not only to a geopolitical project, but also to a geopolitical concept, used by analysts to describe "*the space between the Black and Baltic Seas, which circumscribe it in the north and south, respectively*." (Chodakiewicz, 2012, p. 35) Also, we can observe the term being used as a synonym for the region in the geopolitical analyses of Stratfor and Geopolitical Futures.

The credit for the term goes to Jozef Pilsudski, Marshal and leader of the interwar Poland, who fought for an independent and powerful Poland since his early ages. After achieving this goal in the aftermath of WW1, Pilsudski tried to consolidate the position of the newly-established Polish country, through promoting the project of *Intermarium*, initially as a federation of states, and then as an alliance of states between the two seas. He understood the geopolitics of the region very well and he foresaw that Germany and Russia/Soviet Union would not be weak forever. Hence, the mission of the *Intermarium*, in Pilsudski's vision, was to counter the threats emanating from Berlin and Moscow.[3] The *Intermarium* project, as envisioned by Pilsudski, embraced a pragmatic form, and not a theoretical one. He expressed publicly his vision, which was the product of two factors: his family history and his own bloody experience. (Kaplan, August 14, 2014) His family held lands in the times of the Kingdom of Poland and Grand Duchy of Lithuania. Therefore, his vision would have been a "*spiritual and territorial descendent*" of Polish-Lithuanian Commonwealth, considered to be a Medieval *Intermarium*. (Kaplan, August 14, 2014) He also led the Polish Legions in WW1 and the Polish army in the war against the Soviet Union (1919-1921). (Cambrea, 1939) The cult of Jozef Pilsudski is promoted abroad by Poland. For example, Polish Cultural Institute in Bucharest organized an exhibition for "*a statesman of Poland and of Europe*" (see Figure 1).

[3] This mission was presented at the exhibition "Jozef Pilsudski – om de stat al Poloniei şi al Europei" organized by the Polish Cultural Institute in Bucharest at the Bucharest Municipality Museum (17.04-20.05.2018);



Figure 1: One of the postings presented at the exhibition
"Jozef Pilsudski – om de stat al Poloniei și al Europei"
(Source: Personal Archive)

Both projects failed to be implemented in the inter-war period, due to at least two shortcomings: bad Polish relations with its neighbours (Lithuania and Czechoslovakia) and lack of support from a major power (except for France, who promoted to a lesser extent its *sanitary* cordon). Then Second World War started by splitting Poland between its two powerful neighbours, Nazi Germany and USSR.

Contemporary revival of the *Intermarium* project

With the end of the Cold War, the states from the *Intermarium* region went out of the Soviet sphere of influence, being free to follow an independent foreign and security policy. Most of the states followed the Euro-Atlantic path. The NATO & EU accession of former communist states from Central and Eastern Europe is what Robert Kaplan calls "*the partial institutionalization*" of Pilsudski's idea (Kaplan, 2016, p. 194).

In the wake of Russian aggressions in Georgia (2008) and Ukraine (2014), the idea of *Intermarium* was being promoted again, as a way to solve

the security problems that arise from the East. We do not witness a unitary revival, as one can remark different circles discussing the idea, i.e. academic and political.

The academic revival refers to contributions added by different scholars in developing the theoretical side of the *Intermarium*. First of all, we notice the work of Jan Marek Chodakiewicz, American historian with Polish origins, that lectured on *Intermarium* in 2011 (*Intermarium Lecture Series*) and published the book "*Intermarium: the Land between the Black and Baltic Seas*" (Chodakiewicz, 2017) in 2012. He describes the region in a constructivist manner, defining it as "*an area of coexistence, convergence and clash of many cultures, [that] has historically been a staunch defender of Western Civilization despite long spells of alien domination.*" (Chodakiewicz, 2017, p. 16) Last year, Chodakiewicz reportedly wrote the speech Donald Trump held in Warsaw (July 2017). (Porter, 2017)

In a more pragmatic approach than Chodakiewicz's, George Friedman promoted the idea of *Intermarium* as a new containment line against Russia (Figure 2). One of his articles, published on the 25th of March, 2014 – *From Estonia to Azerbaijan: American Strategy after Ukraine (*Friedman, 2017*)* – became widely popular in the fever of Ukraine crisis. The author believes that while a direct U.S. engagement in Ukraine is not possible, a good strategy would consist in supporting the states that perceive Russia as an enormous threat to their existence. (Friedman, 2017)



Figure 2: *Intermarium* as a new containment line in George Friedman's vision. Source: Stratfor.

Andreas Umland, German researcher based in Kyiv, sees *Intermarium* as the only solution for embedding Ukraine and Georgia into a security structure, as the chances for NATO & EU integration are low (Umland, April 18, 2016).

On the other side, at the political level, we notice the revival of the *Intermarium* project in Poland. The main promoters of *Intermarium* are the current president, Andrzej Duda, and the Law and Justice Party (PiS), which controls both the executive and the legislative. The *Intermarium* idea is attractive to Poland because it implies achieving the status of regional power, which means political, military and economic influence in Central-Eastern Europe. (Hawk, April 26, 2016) In his first speech as president, Duda presented the creation of "*a community of friends*", from the Baltic to the Adriatic Sea, as his main foreign policy goal. ("Duda's inauguration speech", August 5, 2015) In an interview for Polish Press Agency (PAP), the president included the Black Sea in his stated-community. (Smietana, August 23, 2015)

Promoting a foreign policy in line with Pilsudski's idea necessitate a coherent approach, not just political declarations (Szelachowska, January 14, 2016). As the *Intermarium* is a flexible geopolitical idea, today's revival does not imply the creation of a federation of states, but it generates the strategic framework for intensifying cooperation along the North-South axis. There are two emergent formats that contribute to this: the Three Seas Initiative (TSI) and Bucharest 9 (B9).

The Three Seas Initiative

The Three Seas Initiative is, according to the Dubrovnik Statement, "*an informal platform for securing political support and decisive action on specific cross-border and macro-regional projects of strategic importance to the States involved in energy, transportation, digital communication and economic sectors in Central and Eastern Europe.*" ("The Drubovnik Statement", September 2016, p. 7) TSI's goal is to function as an intra-EU lobby format reuniting 12 countries: Austria, Bulgaria, Croatia, Czech Republic, Hungary, Estonia, Latvia, Lithuania, Poland, Romania, Slovakia and Slovenia. The first informal meeting was organized on the sidelines of the 79th session of UN General Assembly, in New York (29th of September 2015). (Bekic and Funduk, 2016, p. 1-2) As a Polish-Croatian initiative, the first two summits were organized in Dubrovnik (August 2016) and Warsaw (July 2017), where it received political support from the United States, through the participation of Donald Trump. Romania joined the nucleus of the initiative and organized the third summit (Bucharest: 17-18 September 2018). This event marked a few concrete steps towards

achieving TSI's goal: the selection of a list of priority interconnection projects, the organization of the first edition of the 3SI Business Forum, the creation of the 3SI Network of Chambers of Commerce and the signing of the Letter of Intent in relation to the establishment of the Three Seas Investment Fund. (*Joint Declaration of the Third Summit of the Three Seas Initiative*, September 18, 2018)

As stated above, a list of 48 new or existing priority projects was selected, at the countries' proposal. There are two types of projects: (1) multilateral and (2) bilateral and national projects with international potential. (*The Three Seas Initiative – Priority Interconnection Projects*)

Table 1 shows the number of projects proposed by every country, which can be interpreted as an expression of their interest for the initiative.[4] Croatia, Poland and Romania have by far nominated the highest number of projects. While Warsaw and Bucharest are keen on multilateral projects, Zagreb has a greater interest in national ones.

Table 1 also shows that Austria, Czech Republic and Latvia do not see TSI as a way to promote certain projects. Almost every proposal involves the participation of other countries, as can be observed in

Table 2 due to geographical position in the middle of the Intermarium, Hungary and Slovakia share the second place, after Croatia and before Poland.

Country	**Multilateral projects**			**Bilateral and national projects with international potential**			**Total**
	Energy (8)	**Digital (8)**	**Transport (11)**	**Energy (6)**	**Digital (2)**	**Transport (13)**	**48**
Austria	0	0	0	0	0	0	0
Bulgaria	0	0	0	0	0	3	3
Croatia	2	1	1	1	1	6	12
Czech Republic	0	0	1	0	0	0	1
Hungary	1	2	2	0	0	0	5

[4] Only a few projects were proposed by 2 or more countries, while the vast majority has a single promoter.

Estonia	0	0	2	2	0	0	4
Latvia	0	0	0	0	0	0	0
Lithuania	2	0	3	1	0	0	6
Poland	2	3	5	0	0	0	10
Romania	1	3	3	0	0	0	7
Slovakia	1	0	0	0	0	2	3
Slovenia	0	0	0	2	1	2	5

Table 1 The number of projects proposed by every country
(Data Source: The Three Seas Initiative – Priority Interconnection Projects)

Country	**Multilateral projects**			**Bilateral and national projects with international potential**			**Total**
	Energy	**Digital**	**Transport**	**Energy**	**Digital**	**Transport**	
Austria	2	7	2	0	0	0	11
Bulgaria	2	6	3	0	0	3	14
Croatia	2	6	3	2	1	6	20
Czech Republic	0	7	3	0	0	1	11
Hungary	4	7	5	1	1	1	19
Estonia	2	5	2	2	0	0	11
Latvia	2	5	2	0	0	0	9
Lithuania	2	5	4	1	0	0	12
Poland	3	7	8	0	0	0	18
Romania	3	7	4	0	0	1	15
Slovakia	4	7	7	0	0	2	19
Slovenia	0	7	2	2	1	2	14

Table 2 The number of participations
in selected projects by every country
(Source: The Three Seas Initiative – Priority Interconnection Projects)

As we can notice from Figure 3, the main energy and transport projects are on the Baltic-Adriatic line: Via Carpathia (Thesaloniki-Klapeida), Via Baltica (Berlin-Warsaw-Kaunas-Riga-Helsinki), Go Highway (Odessa-Gdansk), Rail Baltica, respectively North-South Gas Corridor, LNG terminal in Krk Island (Croatia), bilateral gas interconnectors etc. (Zurawski vel Grajewski, 2017) Although this map dates from 2017 and it does not include two Romanian proposals – BRUA and Rail-2-Sea (Constanta-Gdansk), our 'peripheral' geographic position limits the concrete results for our country.



Figure 3: The main projects to be promoted through TSI.
(Source: Zurawski vel Grajewski, 2017, p. 15)

We subscribe to Liviu Muresan and Alexandru Georgescu's opinion that the Black Sea is the main precondition for the success of TSI, both in

terms of opportunities and source of instability and threats, due to the complex security environment (Mureşan and Georgescu, September-December 2017). The presence of the Black Sea in the TSI's agenda would be in Romania's best interest. It would serve as a way to address the non-military issues from the economic or energetic field, for example.

Dariusz Gora-Szopinski, the chairman of the department of regional strategic studies at the Cardinal Stefan Wyszynski University of Warsaw, believes that TSI has only economic purposes, and so it is a mistake to see it as the revival of the historical Intermarium (Gora-Szopinski, June 2017). Indeed, the mission of TSI is to cooperate in the energetic, transport and digital sector. But this may take place only on the background of a geopolitical shift, i.e. the consolidation of the North-South axis. Moreover, the intensification of cooperation in these areas has significant geopolitical implications, as it makes stronger the states united in their desire to avoid the position of buffer states. As presented above, the flexibility of the geopolitical ideas allow this revival, which is a matter of principles, and not details. Therefore, from a geopolitical point of view, we see TSI as an *extended Intermarium*, due to the inclusion of the Adriatic Sea in the classical form of *Intermarium*.

Bucharest 9 Format

Bucharest 9, the second emergent format that is meant to increase the cooperation in the region and contribute towards developing a North-South axis, from one sea to another, reunites all 9 NATO Eastern Flank countries (Bulgaria, Czech Republic, Hungary, Estonia, Latvia, Lithuania, Poland, Romania and Slovakia). Being formed in November 2015 as a Romanian-Polish initiative before NATO Warsaw Summit (July 2016), B9's purpose is to function as a "*platform for consultation and dialogue*" within NATO. (*The declaration adopted at the final of the first B9 meeting*, November 2015)

Apart from many meetings organized at different levels (Presidents, Ministers of Defence, Ministers of Foreign Affairs, parliamentary summit) either in Bucharest or in Warsaw, concrete steps were also made in the region. First of all, the vast majority of NATO reassurance measures were implemented in the B9 countries: NATO forward presence (eFP – enhanced Forward Presence in Poland and Baltic states; and tFP – tailored Forward Presence in Romania and Bulgaria) (*Boosting NATO's presence in the east and southeast*); the formation of NATO Force Integration Units, which allows quick deployment of troops in case of crisis (Terlikowski et al, 2018). Secondly, 5 of the B9 countries (Romania, Poland and the Baltic states) have already met NATO's defence spending requirement (2% of their GDP on defence), while

the other 4 presented a road map for achieving this target until 2024 (25th of May, 2017) (Terlikowski et al, 2018). Finally, B9 countries launched the modernization of their armed forces, investing into new platforms and weapons, basically from the United States (Terlikowski et al, 2018).

As a consequence of the imbalance between the two forward presences (Socor, 2018), B9 Format may serve as a tool to promote a unitary approach in NATO's deterrence and defence posture.

Conclusions

***Intermarium* – a North-South axis in Central and Eastern Europe:** *Intermarium* is a geopolitical idea (i.e. geopolitical project) and, as every idea of this kind, it is flexible. Having its origins in the interwar period, it is adapted and promoted again at academic and political levels. Nowadays, a North-South axis is rising in the eastern part of Europe. There are two emergent cooperation initiatives that comply with this trend, the Three Seas Initiative and Bucharest 9. Both of them are within the most important pillars for European security and prosperity, the European Union, respectively the North Atlantic Treaty Organization.

The revival of the *Intermarium* is not only about creating a common and stronger voice within the EU and NATO, but also about a quest for regional (informal) leadership. Romania, as a core member of both formats, must be very active, through organizing events (meetings or summits) that increase our international visibility, respectively by implementing concrete projects. As it is revitalized today, *Intermarium* is a chance for Romania to be the southern pillar of the emerging North-South axis in Central-Eastern Europe.

References:

1. Brzezinski, Zbigniew, (2000), *Marea Tablă de Șah. Supremația americană și imperativele ei geostrategice*. București: Editura Univers Enciclopedic.
2. Cambrea, Nicolae, (1939), *Mareșalul Pilsudski: Omul de stat și comandantul supreme al forțelor poloneze în Războiul polono-rus din anul 1920*. Brașov: Institutul Cartografic Unirea.
3. Dobrescu, Paul, (2003), *Geopolitica*. București: Editura Comunicare.ro.
4. Friedman, George, (2009), *The next 100 years: A Forecast for the 21st Century*. New York: Doubleday.
5. Hlihor, Constantin, (2005), *Geopolitica și Geostrategia în analiza relațiilor internaționale contemporane*. București: Editura UNAp „Carol I".

6. Kaplan, Robert, (2016), *In Europe's Shadow: Two Cold Wars and a Thirthy-Year Journey through Romania and beyond*. Random House Publishing Group.

7. Kaplan, Robert, (2010), *Monsoon: The Indian Ocean and the Future of American Power*, Randam House Publishing Group.

8. Kaplan, Robert, (2014), *Răzbunarea Geografiei. Ce ne spune harta despre conflictele viitoare şi lupta împotriva destinului*. Bucureşti: Editura Litera.

9. Marek Jan Chodakiewicz, (2012), *Intermarium: The Land Between the Black and Baltic Seas*, Transaction Publishers.

10. Sempa, Francis P., (2002), *Geopolitics: from the Cold War to the 21st century.* New Brunswick: Transaction Publishers.

11. Serebrian, Oleg, (2006), *Dicţionar de geopolitică*. Iaşi: Editura Polirom.

12. Thucydides, (1966) *Războiul Peloponesiac*, Ed. Ştiinţifică şi Enciclopedică, V. 89.

13. "The Drubovnik Statement" on the Three Seas Initiative, (September 2016) Newsletter of the Office of the President of the Republic of Croatia, No. 6, p. 7. Available at http://predsjednica.hr/files/NEWSLETTER%20VIEWS%20and%20NEWS_no%206.pdf and accessed on 22.02.2018.

14. Bekic, Janko, and Marina Funduk, (2016), The Adriatic-Baltic-Black Sea Initiative as the revival of "Intermarium". Brief, Zagreb: Institute for Development and International Relations (IRMO).

15. Friedman, George, (2017), *From Estonia to Azerbaijan: American Strategy after Ukraine*. Stratfor. Available at https://worldview.stratfor.com/article/estonia-azerbaijan-american-strategy-after-ukraine and accessed on 14.01.2018.

16. Gora-Szopinski, Dariusz, (07.06.2017), *Trimarium is not Intermarium*. Available at http://neweasterneurope.eu/2017/07/06/trimarium-is-not-intermarium/ and accessed on 27.11.2017.

17. Hawk, J., (26.04.2016), "EU DEATH WATCH, PART 1: "INTERMARIUM"." South Front. Available at https://southfront.org/Intermarium-a-hare-brained-scheme-whose-time-has-come/ and accessed on 12.12.2017.

18. *Joint Declaration of the Third Summit of the Three Seas Initiative*, (18.09.2018). Available at http://www.presidency.ro/ro/media/comunicate-de-presa/joint-declaration-of-the-third-summit-of-the-three-seas-initiative and accessed on 19.09.2018.

19. Kaplan, Robert, (14.08.2014), "Pilsudski's Europe." Stratfor. Available at https://www.stratfor.com/weekly/pilsudskis-europe and accessed on 12.01.2018.

20. Muresan, Liviu and Georgescu, Alexandru, (Sept-Dec. 2017), *A Romanian Perspective on the Three Seas Initiative.* The Market for Ideas. No. 7-8. Available at http://www.themarketforideas.com/a-romanian-perspective-on-the-three-seas-initiative- a314/ and accessed on 20.08.2018.

21. NATO website. Boosting NATO's presence in the east and southeast. Available at https://www.nato.int/cps/en/natohq/topics_136388.htm and accessed on 22.05.2018.

22. Poland's Presidency website, (05.08.2015), "Duda's inauguration speech". Available at http://www.president.pl/en/news/art,7,address-by-the-president-

of-the-republic-of-poland-mr-andrzej-duda-before-the-national-assembly.html and accessed on 14.09.2017.

23. Porter, Tom, (06.07.2017), "Did a Polish Far Right Activist Help Donald Trump Write His Speech in Warsaw." Newsweek. Available at http://www.newsweek.com/poland-trump-anti-semitism-632702 and accessed on 22.02.2018.

24. Smietana, Mariola, (23.08.2015), "The revival of Intermarium?" Visegrad Plus. Available at http://visegradplus.org/opinion/the-revival-of-Intermarium/ and accessed on 10.10.2017.

25. Socor, Vladimir, (2018), *NATO's Summit Takes Half-Way Measures on the Black Sea Region (Part One).* The Jamestown Foundation. Eurasia Daily Monitor. Volume: 13. Issue: 128. Available at https://jamestown.org/program/natos-summit-takes-half-way-measures-on-the-black-sea-region-part-one/ and accessed on 14.02.2018.

26. Szelachowska, Ksenia, (14.01.2016), "The revival of Intermarium - Poland can talk the talk but can it walk the walk?" Stratfor. Available at https://www.stratfor.com/the-hub/revival-Intermarium-poland-can-talk-talk-can-it-walk-walk and accessed on la 12.12.2017.

27. Terlikowski et al., (08.06.2018), PISM Policy Paper no. 4 (164): The Bucharest 9: Delivering on the Promise to Become the Voice of the Eastern Flank. Available at http://www.pism.pl/files/?id_plik=24501 and accessed on 09.06.2018.

28. *The declaration adopted at the final of the first B9 meeting*, November 2015 ("Declarația comună „Solidaritatea Aliată și Responsabilitatea Comună"). Available at http://www.presidency.ro/ro/media/comunicate-de-presa/declaratie-comuna-privind-solidaritatea-aliata-si-responsabilitatea-comuna and accessed on 25.04.2018.

29. The Institute of World Politics, *Intermarium Lecture Series*. Available at https://www.iwp.edu/events/page/Intermarium-lecture-series and accessed on 22.03.2018.

30. *The Three Seas Initiative – Priority Interconnection Projects*. Available at http://three-seas.eu/press-releases/#e52128e17o and accessed on 20.09.2018.

31. Umland, Andreas, (April, 2016), "Countering Russian Expansionism: Blueprints for a New Security Alliance." European Council for Foreign Relations. Available at http://www.ecfr.eu/article/commentary_countering_russian_expansionism_blueprints_for_a_new_security_al and accessed on 10.10.2017.

32. Zurawski vel Grajewski, Przemyslaw, (2017), "Trimarium: A View from the North." Adriatic-Baltic-Black Sea: Visions of Cooperation. Warsaw: Institute for Eastern Studies.

RECONFIGURING THE BALANCE OF POWER IN THE WIDER BLACK SEA REGION: THE ROMANIAN PROPOSAL FOR AN ALLIED NAVAL COOPERATION

Adrian-Vasile POPA*

Abstract

The de facto annexation of Crimea in March 2014 and its subsequent militarization with Russian anti-access / area denial capabilities represent a game changer for the security environment in the Wider Black Sea Region. By claiming large parts not just of Crimea's, but also of Ukraine's continental shelf and Exclusive Economic Zone, Russia may significantly change the balance of power in the region. Facing the probability of sharing volatile frontiers with Russia, the riparian states have responded through various initiatives that would allow the strengthening of their military positions. Such an attempt is the Romanian proposal for a Black Sea naval cooperation with Turkey and Bulgaria under the NATO umbrella. This initiative is at a standstill as of 2018 despite NATO launched a multinational Black Sea force headquartered in Craiova (Romania) last year that is expected to include additional sea assets to those already existent, namely sporadic NATO naval patrols. Indeed, Russia suggested that the aforementioned proposal may establish the premises for a permanent NATO Black Sea Fleet that infringes upon the provisions of the Montreux Convention and could constitute a veritable casus belli. This paper follows the itinerary of the Romanian initiative, analyzes the strategic and operational challenges that it is facing in the light of the Montreux Convention and not ultimately, offers possible prospects for a permanent NATO Black Sea Fleet.

Keywords: *Annexation of Crimea, Black Sea, Montreux Convention, NATO, Russia.*

Introduction

The tough competition between the two superpowers of the Cold War era – the United States and the Soviet Union – had apparently ceased after the

* Opinions expressed by the author are his own views and they do not reflect in any way the official policy or position of "Mihai Viteazul" National Intelligence Academy. PhD Candidate, "Mihai Viteazul" National Intelligence Academy, Romania, email: adrian.popa@animv.ro

fall of the Berlin Wall in 1989 and gave F. Fukuyama good odds for the prediction made in his 1992 book, *The End of History and the Last Man*, on the universalization of Western liberal democracy as the final form of human government. This ultimate development will eventually lead to the accomplishment of the democratic peace theory which stipulates, in general terms, that a democracy does not engage in an armed conflict with another democracy; thus, the achievement of a perpetual global peace being assured. However, the recent military developments in the Wider Black Sea Region (WBSR) seem to give more credit to the offensive realism theory postulated by J. Mearsheimer. From the perspective of this famous representative of the neorealism school of thought, even though a Great Power does not have the means to acquire hegemony, it still acts in an offensive manner to secure as much power as possible because states are in almost all cases in a better situation when they have more power compared to when they have less. As a consequence, the current anarchic international stage is provoking a permanent security competition between states (Mearsheimer, 2001). Therefore, in the light of the offensive realism theory, two major strategic maneuvers of the Euro-Atlantic structures in the WBSR entered in competition with Russia's ambition to regain its Great Power status in the post-Cold War era.

Firstly, NATO's expansion beyond the borders of a reunified Germany could have made Russia "a victim of the encircling of the Eurasian heartland by thalassocratic powers" (Barna, 2014, p. 32). Assuming the loss of hegemonic influence on the Baltic states and the subsequent concessions made to these states to join NATO as a never again compromise inherent to the process of transition from the USSR, the Kremlin was confronted with a potential repetition of this scenario during the 20th NATO Summit held in Bucharest in 2008. Back then Ukraine and Georgia were expecting to be offered NATO Membership Action Plan – a prelude to full membership (Harding, 2008). However, the 23rd point of the Bucharest Summit Declaration was only assuring these countries that they were going to receive this status (NATO, 2008). The timing obtained by Russia, considered by some political analysts as "the biggest foreign policy victory of Mr Putin's presidency" (Blomfield and Kirkup, 2008), proved to be decisive in the case of Ukraine and Georgia's aspirations for NATO membership as subsequent Russian military interventions in the above mentioned countries undermined their prospects for such a geopolitical endeavor - as of 2018, Ukraine and Georgia's chances to join NATO seem to be close to zero.

Secondly, the Eastern expansion of the EU as part of its *Wider Europe* project (for details, see Commission of the European Communities, 2003) did

not take into account Russia's interests in the region, but rather dismissed them. As a consequence, it became a rival of the *Greater Europe* project (for details, see Kortunov, 2018) that envisaged a stronger Russian influence on the European continent. Indeed, as Freire (2017, p. 19) noticed, "As much as the EU project includes a stable and prosperous neighbourhood where security dynamics will positively impact the Union's security, Russia also sees security and friendship at its borders as promoting its own security. The clashing projects of the EU and Russia towards this area of common interest, but where the projection of distinct interests is clear, led to a fundamental division". The clashing projects resulted in various conflict epicenters in Eastern Europe provoked by Russia. By creating instability at the EU's doors, Russia intended to deter the advance of the former's *Wider Europe* project in Eastern Europe and to warn the affected states that they still need to consult with their hegemon when taking major decisions in terms of national security and foreign policy.

These strategic maneuvers could not be tolerated anymore in the recent years by the Kremlin. As a consequence, starting with his first presidential mandate in 2000, Putin began to amplify the nationalism of his compatriots by projecting an ideological enemy that was so well-known to most of the Russian citizens confronted with Soviet nostalgia – an expansionist west, full of immoral values and ready to divide and conquer their millennial Orthodox civilization. Based on the US denouncement of improved relations with Russia within the framework of Obama administration's initiative of 2009 known as *the Russian reset*, Putin stated very clearly in his *Crimean speech* of March 2014 that "in short, we have every reason to assume that the infamous policy of containment, led in the 18th, 19th and 20th centuries, continues today. They [NATO and the EU] are constantly trying to sweep us into a corner because we have an independent position, because we maintain it and because we call things like they are and do not engage in hypocrisy. But there is a limit to everything" (The Kremlin, 2014). Definitely, the geostrategic developments of the new millennium – mainly concerning NATO and the EU's expansion to the former Eastern Bloc – along with the emerging approach of the West to Russia as a regional power, crossed the limit referred to above. Indeed, it was clearly stated in the *Russian National Security Strategy* of December 2015 that "the buildup of the military potential of the North Atlantic Treaty Organization (NATO) and the endowment of it with global functions pursued in violation of the norms of international law, the galvanization of the bloc countries' military activity, the further expansion of the alliance, and the location of its military infrastructure closer to Russian borders are creating a threat to national security" (The

Kremlin, 2015). As a consequence, from case to case, by using military force in a direct (e.g. the Russo-Georgian War of August 2008) or an indirect (e.g. military support offered to separatists in Donbass starting with early of 2014) manner, along with the use of economic pressure (e.g. Russia-Ukraine gas disputes originating in 1992, moderated from time to time by Ukraine's concessions over the lease of Sevastopol until the annexation of Crimea in March 2014 by Russia) and of other soft-power instruments (e.g. support offered to the Party of Communists of the Republic of Moldova and to its ideological successors such as the Party of Socialists of the Republic of Moldova), Russia managed to maintain not only its position as the leader of the WBSR, but also reinstated its status as Great Power with global outreach.

Most of these still ongoing strategic clashes between the Euro-Atlantic structures and Russia have common scenery: the Black Sea and, by extension, the WBSR. Apart from Russia, the rest of the Black Sea riparian states are either NATO members (Turkey, Romania and Bulgaria) or partners (Georgia and Ukraine). In addition, Romania and Bulgaria are also EU members, Turkey has an uncertain EU candidate state status, Georgia and Ukraine are members of the Eastern Partnership meanwhile Russia is a contested strategic partner of the EU in the light of this country's annexation of Crimea and its involvement in the War in Donbass (European Parliament Press Releases, 2015). Being an isolated body of water, the Black Sea is connected to the international maritime routes through two narrow Turkish Straits – Bosphorus that connects it with the Sea of Marmara; and Dardanelles that further connects the latter with the Aegean and Mediterranean Seas. The access of the naval vessels in or out of the Black Sea is strictly regulated under the provisions of the Montreux Convention of 1936.

The Black Sea was a relative-low stake issue in the public agenda of international politics for more than a decade after the end of the Cold War. However, the high-impact of 9/11 on the global security architecture and the two major strategic maneuvers of the Euro-Atlantic structures in the WBSR - discussed above -, doubled by Russia's repositioning on the global stage, drew the international attention to the Black Sea and made it, in recent years, probably the most visible area of on-going geostrategic experiments. On the one hand, as Lucinescu pointed out, "the Wider Black Sea Region is extremely important for the Euro-Atlantic community because, along with the Mediterranean Sea, it can form a 'safety zone' to protect the European pillar of the Alliance from the major conflict outbreaks in Maghreb, the Middle East and the Caucasus area. At the same time, the western shore of the Black Sea has provided, in the last years, excellent bases of projection of military forces in the Middle East war zone, where NATO was actively involved in the last

decade" (2016, p. 4). On the other hand, the Black Sea is very important for the EU as well because most of its members rely on energy sources originating from or at least transiting this region. In addition, the Black Sea witnessed the newly-emerged challenges to the European security – such as nuclear proliferation, frozen conflicts, terrorism or the seemingly uncontrollable waves of refugees – which coupled with the dramatic shift of the US strategic interests away from Europe for more than a decade after the end of the Cold War, put pressure on the Europeans to share in the responsibility for global security in order to ensure their own integrity. Overall, NATO and the EU have not agreed so far on a common strategic vision for the Black Sea, mainly because of their different perception on the intensity of the threats. As Lucinescu remarked, the EU aims to create a circle of friends within its Eastern neighborhood meanwhile NATO rather promotes a dual concept of brigde-barrier for the region (2011, p. 90). From another perspective, the Black Sea is a common place for Russian history, still being a stronghold of geostrategic importance for this country (see Toucas, 2017), meanwhile Crimea plays a central role within this equation (Figes, 2014). Indeed, as Renz and Smith revealed "from the point of view of Russia, the country could not be 'sovereign' under the post-Cold war consensus. In order to ensure Russian 'sovereignty' (greatpowerness), a shift in the international balance of power was seen as inevitable" (2016, p. 21).

The annexation of Crimea and its subsequent militarization with Russian A2/AD – a game changer for the WBSR

The above-mentioned shift in the international balance of power – which also represents on this particular case a veritable game changer for the security environment in the WBSR – was materialized in March 2014 through the *de facto* annexation of Crimea and its subsequent militarization with Russian anti-access / area denial (A2/AD) capabilities. As indicated in my previous conference paper entitled *The Twofold Outcome of Russia's Hybrid Warfare in Ukraine*, the trigger of this outcome was the organization of an alleged referendum in Crimea on 16 March 2014 by ethnic Russians – dissatisfied with the overthrow of Yanukovych in the light of the *Ukrainian Revolution* of February 2014 – whose result cleared the way for the Russian military intervention in the region on the basis of protecting the rights of Russian nationals abroad (the Kosovo precedent was claimed as well) and subsequently lead to Putin's official approval for the incorporation of the Republic of Crimea and the city of Sevastopol into the Russian Federation on 18th of March 2014 (Popa, 2018, p. 15). In addition, the same article claims

that the current strategic objectives pursued by Russia when controversially enlarging its territory by annexing Crimea are to ensure Russia's control over the Port of Sevastopol and by extension safeguard its vital strategic interests in the WBSR. In this sense, some interconnected benefits for Russia can derive from this strategic maneuver: a newly-acquired capacity of global power-projection based on the independent-control of the Port of Sevastopol; a leverage for controlling navigation and protecting its communication lines and energy transportation routes in the Black Sea maritime space; an increased capacity to impede not only the energy diversification strategy of Ukraine, but also the potential of similar projects in the Black Sea foreseen by the other riparian states; and an unofficial subsidy for the Russian criminal networks to relocate their stronghold from the Port of Odessa to the Port of Sevastopol as the latter can offer lower transit costs and new trafficking routes meanwhile being assured in terms of security by the Russian Black Sea Fleet based there (Popa, 2018, p. 16-18). In addition, the annexation of Crimea without local resistance as a result of the almost overnight Ukrainian service personnel of Crimea's defection, a masterpiece of the Kremlin's propaganda in the recent years, was used on three levels: at national level, it consolidated Putin's leadership ahead of the Russian presidential elections of 2018; at regional level, it signalled the neighbouring countries formerly belonging to the Soviet Union's sphere of influence and encompassing nowadays a considerable number of Russian ethnics that the strenghtening of their connections with the Euro-Atlantic structures is immediately condemned and strictly punished by Moscow; and at global level, it demonstrated that Russia needs to be treated as an equal interlocutor by the West at least when it comes to projecting security in the WBSR.

The annexation of Crimea has also provided Russia with an exquisite military infrastructure. Indeed, by citing the Ukrainian Ministry of Defence, Daly revealed that "in addition to Sevastopol, the finest natural harbor in the Black Sea, Russia also acquired the former Crimean Ukrainian naval bases of Novoozerne on Donuzlav Bay, Myrnyi (Donuzlav Lake), Saky, Balaklava and a marine infantry base at Feodosiia" (2014). In any way, the main military platform seized was the Port of Sevastopol whose control was regained in the post-Cold War era by Russia as a result of Boris Yeltsin's agreement on the 1997 Black Sea Fleet Partition Treaty that established both the sum required to be paid by Russia for stationing its Black Sea Fleet at Sevastopol and the value of the compensation given to Ukraine for its part of the Soviet divided fleet; and of the update of this agreement in 2010 when Dmitry Medvedev signed the Kharkiv Pact which acknowledged the exchange of the sum of the lease for a discounted price for Ukraine's import of Russian natural gas.

Indeed, according to Alan Yuhas and Raya Jalabi, Sevastopol has been used by Russia even before the annexation of Crimea as an important hub to project Russia's naval power on a global platform as it has proved its efficiency during the Black Sea Fleet staged blockades in the 2008 Russo-Georgian War and during the Syrian civil war when the Port of Sevastopol served as an alternative for the temporary inaccessibility of the Port of Tartus (2014). In this sense, the annexation of Crimea valued even more in the equation of Russia's power projection at the Black Sea as "the takeover of Crimea not only eliminates the need to pay these fees, but Russia gains an opportunity to modernise the Fleet in any way it sees fit, which so far had been limited by the Russian-Ukrainian agreement which only provided for the possibility of renovating the equipment that was already there (Olszanski et al, 2014)".

The accelerated modernisation of the newly-acquired military infrastructure of Crimea has started since 2014 under the authority of Sergey Shoigu, the current Russian Minister of Defence, and transformed the peninsula in a veritable strategic *place d'armes* in the Black Sea. There is a long list of high-end military equipments deployed by Russia in Crimea after the annexation of the peninsula. Some of these deployments are officialy confirmed by the Kremlin meanwhile the others are still having a speculative status – statements launched in this sense by policymakers, military experts and scholars should be treated with caution as they can actually represent fake news used by the belligerent parties through various channels of propaganda in the light of the ongoing War in Donbass and of the unsettled legal status of Crimea. For example, Celac et al. mentioned that the Soviet ships have largely been modernized, and reinforced with two Admiral Grigorovich-class guided missile frigates. Additionally, the Russian Navy has expanded its submarine flotilla in Sevastopol, with the addition of four to six 'Improved' Kilo-class submarines (...) A squadron of Su-30SM's provides air cover, while an Su-24 detachment offers Russian commanders a long-range antiship and anti-ground platform (2016, p. 8). In addition, J. Wade of the international security blog *Conflict Observer* announced that new Podsolnukh over-the-horizon radar could be installed in Crimea enabling the detection of any foreign ship passing through the Bosphorous Strait in Turkey and as for anti-ship capabilities, the K-300P Bastion-P is already deployed around Sevastopol to protect docked warships (2017). Even more, Ukraine's Ministry of Temporarily Occupied Territories and Internally Displaced Persons has recently issued a public statement announcing that, as of late September 2018, the anti-aircraft missile Systems S-400 *Triumf* have been deployed by Russia near the cities of Sevastopol, Feodosia and Yevpatoria (2018). From another perspective, the inauguration in May 2018 of the Crimean Bridge over the

Kerch Strait– an infrastructure development aimed to fully cut the Crimean Peninsula off from mainland Ukraine by creating a land connection between the former and Russia's Krasnodar region –offers Russia control of the both sides of the Kerch Strait meanwhile allowing this country to supply with resources the newly-annexed territory.

As a result, the new Russian military developments in Crimea had a direct impact on both the efficiency of the ground force, navy, air force and air defence units and the quality of the existent infrastructure; this multifaceted capacity led to the creation of an efficient A2/AD around the Crimean Peninsula. According to Anastasov of *NATO's Political Affairs and Security Policy Division*, "Anti-Access/Area Denial (A2/AD) is a military jargon to describe the situation when a state deploys weapons systems, often with long-range capabilities, to deny foreign forces freedom of movement in the theatre. Land-based surface-to-air missiles, surface-to-surface ballistic or cruise missiles, and anti-ship missiles are the capabilities most often used for building up A2/AD. Additional elements may be added to the system for example: advanced aircrafts, surface ships and submarines" (2018). As an extension, the A2/AD in Crimea is strengthened by a Russian-fuelled high-intensity hybrid warfare – "a form of violent conflict that combines a range of different dimensions of war (military, economic, information and cyber), tactics (regular and irregular) and actors (state and non-state)" (Scheipers, 2016, p. 47). In this sense, the operationalization of the A2/AD around the Crimean peninsula adds to the already existent Russian A2/AD system encompassing military deployments from the Arctic region down to Syria, with a high-density in the Kalinigrad Oblast. According to Jankowsky, "Russia's A2/AD systems are important for two other reasons. First, a leaner chain of command and streamlined decision-making system mean Russia can act much faster than NATO allowing it to achieve escalation control. Second, nuclear weapons remain a crucial element of Russia's escalation dominance strategy. In a situation when allied forces would consider breaking through Russia's A2/AD system, Russia could threaten to use its nuclear capabilities as a deterrent (...) Through this approach, Russia can control the level of conflict escalation, dominating the mechanism and circumstance of escalations where nuclear elements play a fundamental role" (2018). The amplitude of these recent military developments in Crimea suggests that the A2/AD systems employed there have not only a defensive posture, but an offensive potential as well. Indeed, as Celac et al. remarked "Russia couples its naval superiority in the Black Sea with growing political and military influence in the surrounding states (…) Increasing political power combined with a strong military position make Russia the virtual regional hegemon at this point

(2016, p. 17)". Indeed, the potential Western perception of the Black Sea as a *Russian lake* is very dangerous as it implies long-term effects on the Eastern European countries, similar to those of the Iron Curtain during the Cold War. According to Socor, "such a perception could eventually lead to: sealing the occupation of territories from Georgia, Ukraine, and Moldova as permanent Russian gains; re-admitting Russia into 'regional' (i.e., limited to riparian countries) security arrangements, in which Russia would no longer be Turkey's equal but would far exceed Turkey's power; and turning Russia into an arbiter of energy markets and pipelines in a number of European destination countries far beyond the Black Sea" (2018). Therefore, as it can be seen below, the recent transformation of Crimea into a military stronghold threatening the security and stability in the WBSR could not remain without a reaction from the stakeholders of the region.

Consequences of Crimea's recent militarization and the stakeholders' reaction

According to J. Mearsheimer, the security dilemma reflects the basic logic of offensive realism. The essence of this dilemma is that measures taken by a state to increase its own security generally lead to diminishing the security of other states (2001, p. 30). From this perspective, the most affected country by Crimea's recent militarization under the *de facto* Russian authority is by default Ukraine. In addition to the loss of territory, of a series of implicit civilian and military assets and of real perspectives to join the Euro-Atlantic structures discussed above, Ukraine is also affected on two dimensions by the questionable legal status of the maritime space around the Crimean Peninsula. Firstly, in terms of trade, the militarization of Crimea coupled with the operationalization of the Crimean Bridge have a dramatic economic impact on the Ukrainian region of Donbass – this region is already impoverished since its 2014 split between the Ukrainian government and the self-proclaimed Donetsk and Luhansk People's Republics (DPR, respectively LPR). According to R. B. Urcosta of *The Jamestown Foundation*, "Moscow's de facto control of both sides of the Kerch Strait, combined with its activities that limit freedom of navigation for Ukrainian vessels there, essentially turn the Azov Sea into a 'Russian lake'. As such, Russia is progressively pushing to deprive Ukraine of its economic and political sovereignty in and around the Azov Sea" (2017). Adding insult to injury, DPR has created since 2015 its own so-called flotilla at the Azov Sea (see OstroV, 2016). As a result of these actions, the trade turnover for example in Mariupol, Ukrainian city confronted with an already delicate social situation since 2014 and which is heavily dependent on its

ability to export Ukrainian steel to international markets, is anticipated to fall by 25–30 percent (Kabanenko, 2017). Secondly, in terms of energy – considered as both the subsoil resources of the Black and Azov Seas and the energy routes crossing this maritime space from the Caspian Sea on their way to the European continent – the loss of Crimea is synonymous with the reduction in size of Ukraine's continental shelf and Exclusive Economic Zone (EEZ). According to Olszanski et al, the loss of Crimea practically negates the possibility of Ukraine implementing projects to extract hydrocarbons from the Black Sea shelf which it had planned jointly with Western companies (2014). In addition, Russia even proposed in 2016 a new energy route through Crimea for the building of South Stream (Novinite, 2016). Even though the South Stream project is obsolete as of October 2018, this proposal reveals Russia's intention to fully-exploit the Crimean's maritime space. Indeed, the operationalisation of the TurkStream – a natural gas pipeline currently under construction from Russia to Turkey – diminishes the necessity of transiting the Russian gas to Europe via Ukraine. Even though Vladimir Putin assured in May 2018 that Russia would not halt the transit of gas through Ukraine if this remained cost-effective (Sputnik, 2018), it is almost a certitude that the operationalisation of TurkStream and Nord Stream 2 – a natural gas pipeline currently under construction from Russia to Germany via the Baltic Sea – will drastically reduce the current transit revenues collected by Ukraine.

The Black Sea riparian states have also been affected directly, in terms of trade and energy, by the annexation of Crimea – at a lower intensity though compared to Ukraine.As Russia's annexation of Crimea is not recognized by the rest of the Black Sea riparian states, this situation creates volatile borders. For Romania, Russia's intention over the newly-obtained EEZ around the Crimean Peninsula is highly important since it was only in 2009 that the International Court of Justice settled its dispute with Ukraine regarding the EEZ around Serpent's Island, an area on which Russia may express its interest. Therefore, Romanian's victory of 2009 can be partially invalidated by the annexation of Crimea. As Joja put it, now that Romania and Russia are maritime neighbours, bilateral disputes are far more likely. In this sense, Russia has the capacity to obstruct explorations, force the withdrawal of Romanian companies, block commercial flow from the Danube River to the Black Sea, or even attack Romanian capabilities in the Exclusive Economic Zone (2018). Bulgaria is also concerned about disruption to maritime trade routes because, as Bugajski and Doran indicate, 80% of this country's imports and exports are shipped via the Black Sea (2016, p. 3). Nevertheless, the biggest Russian threat remains the military one. Numerous incidents both in air and on sea have been periodically reported since 2014 as a result of the

questionable delimitation of the Black Sea's maritime and air space. Probably the most alarming one happened in January 2018 when an armed Russian Su-27 jet performed an unsafe intercept of a US Navy EP-3 surveillance plane, flying within 5 feet of the US military aircraft, in order to prevent the US plane from entering a claimed Russian airspace near Crimea (Browne, 2018). In addition, the potential offensive posture of the Russian A2/AD can provoke nightmares for the policymakers of the riparian states. According to some unconfirmed Ukrainian reports of this year (UNIAN, 2018), Russia has already deployed advanced nuclear-capable missiles Iskander which can easily reach the shores of the riparian states and cause devastating effects. Likewise, even though the hybrid warfare supposedly perpetrated by Russia in the WBSR has more subtle effects, it can certainly cause high damage for the Black Sea riparian states. Anastasov confirms that "the entire region, down to each individual country, is weaker, less open for integration and dangerously prone to subversion. A regular instrument of choice is the spread of fake news and conspiracy theories, many of which suggest a hidden Western agenda. More often the aim is to fuel anti-establishment grievances, including direct support for political parties with anti-NATO agendas and anti-European agendas, feeding Euro-skepticism at large" (2018). As a consequence, facing the probability of sharing volatile frontiers with Russia, the riparian states have responded through various initiatives that would allow the strengthening of their military positions. In general terms, this reaction was grouped under the frameworks of the Euro-Atlantic structures. While the EU plays a more civil role in enforcing the security of the Black Sea riparian states by promoting the rule of law and good governance, NATO remains the only viable coagulator of the military initiatives at the Black Sea aimed to strengthen the position of the riparian states as a result of Crimea's recent militarization.

NATO's main contributor, the United States, has developed military bases in the Black Sea riparian states since the Cold War – e,g, the Incirlik Air Base and Izmir Air Station, both on Turkish land. Subsequently, the United States multiplied them at the same time with NATO's formation of the Southern part of its Eastern flank, by using Romania's infrastructure such as Mihail Kogalniceanu Air Base, Babadag training base, Smardan training area, Cincu training area and the recently-become operational AEGIS Ashore missile defence facility in Deveselu; and Bulgaria's Aytos Logistics Center, Novo Selo Range, Bezmer Air Base and Graf Ignatievo Air Base. However, NATO as a collective defence organization focused on the importance of the military positions of the Black Sea riparian states only after 2004 when Romania and Bulgaria joined as new members. This development was very slow and it was activated only as a reaction aimed to mitigate the effects of an existent crisis.

Indeed, two major events on the shores of the Black Sea during the post-Cold War period intensified NATO's appetite to ensure security in the region: firstly, the Russian aggression against Georgia in 2008 made NATO send its Standing Maritime Group One to conduct port visits and joint exercises with Romania and Bulgaria – as revealed by Kramer, this action was condemned overtly by Russia as a violation of the Montreux Convention (2008); and secondly, Russia's annexation of Crimea in 2014 provoked NATO to consolidate its South-Eastern flank by forming a Tailored Forward Presence in the Black Sea (Reuters, 2017).

From another perspective, the Black Sea riparian states have also proposed initiatives to enhance the military cooperation at regional level, without a compulsory prerequisite for NATO framework. Even though some of them were operationalized – such as *Black Sea Harmony* or *BLACKSEAFOR* –, these initiatives had modest results in terms of strengthening friendship and good neighborly relations among the Black Sea riparian states, mainly because of Russia's destabilizing activities in the region – this state being a member of these military developments. However, the most promising initiative still waiting for its operationalization as of 2018 remains the Romanian proposal of 2016, discussed below, aiming to create the premises for an enhanced Black Sea naval cooperation with Turkey and Bulgaria.

The Romanian proposal for an enhanced naval cooperation with the other Black Sea riparian states NATO members

Romania has been promoting the importance of ensuring security at the Black Sea long before Russia's annexation of Crimea. It was in the interest of Bucharest to establish and consolidate the presence of the Euro-Atlantic structures within the region as a way of ensuring its own security. According to *Romania's National Defense Strategy 2015-2019*, the national security objectives pursue – among others – ensuring security in the Black Sea region; deepening cooperation with neighboring states and states of NATO's Eastern flank; and intensifying regional cooperation, including in the field of defense (2015, p. 10). As a consequence, in the light of its assumed national security objectives coupled with Russia's destabilising activities at its borders, Romania's proposal to Turkey and Bulgaria, in the preparation of the Warsaw Summit of July 2016, for a Black Sea enhanced naval cooperation under a non-compulsory NATO umbrella – i.e. the cooperation could have been conducted at trilateral level, possibly in a NATO context – came as a natural action. Mihnea Motoc, a Romanian diplomat who has served as Minister of Defence between November 2015 and January 2017, announced in April 2016 the

launch for consultation of this initiative envisaged as a platform for enhanced naval cooperation between the NATO members of the Black Sea that would allow – based on constant exercises – the existence of an almost permanent Allied naval presence in the region, in full compliance with the Montreux Convention. In addition, the high-ranking official announced that this initiative will be open for the Black Sea members of the Eastern Partnership – Georgia and Ukraine – as well as for the non-Black Sea members of NATO such as the United States (Pantazi, 2016).

A series of bilateral meetings were conducted by the mentioned Romanian defense minister and acting Romanian foreign affairs minister at the time, Lazar Comanescu, with their Bulgarian counterparts in order to reach a consensus regarding the political and military parameters of this initiative. Bulgaria's initial responses appeared to be positive since at the time Bulgarian President Rosen Plevneliev endorsed it publicly during his Romanian counterpart Klaus Iohannis's visit to Sofia in mid June 2016 by expressing his acknowledgement on the Bulgarian defense minister Nikolay Nenchev and Bulgarian foreign affairs minister Daniel Mitov's initial consent of the Romanian initiative (President of Romania – Press statements, 2016). However, a dramatic shift in the Bulgarian stance emerged during the same visit of Romania's president in Bulgaria. Being alarmed by a potential lack of a NATO flag for this initiative and assessing the risks of Russia's retaliation over his country as a result of the operationalisation of this trilateral initiative – i.e. with or without a NATO flag –, the Bulgarian Prime Minister Boyko Borisov appeared at a joint press conference with Plevneliev calling for the revoke of the preliminary consent. Borisov was justifying his decision as "I always say that I want the Black Sea to see sailboats, yachts, large boats with tourists and not become an arena of military action (...) I do not need a war in the Black Sea" (cited in Reuters, 2016). Even though Plevneliev, Nenchev and Mitov moderated their opinion regarding the Romanian initiative, they were still favourable to it ahead of the Warsaw Summit as long as it was implemented in a NATO format and not as a trilateral initiave possibly seeking at an unknown date a NATO mandate (see Bulgarian News Agency, 2016). This was not the case of Borisov who maintained his position up until the Warsaw summit. Yordan Bozhilov, the President of *Sofia Security Forum* and Manager of Programs *South East Europe and Black Sea* reveals some methods of Russia's potential blackmail that might have forced the Bulgarian prime minister to reject the Romanian initiative: "A few days prior to the visit of the Romanian President in Bulgaria it became clear that Sofia will have to pay the Russian company 'Atomstroyexport' EUR 550 million for commissioned but undelivered equipment for the construction of a second nuclear power plant

in Bulgaria (...) Furthermore, Bulgaria is very much dependent on Russian supplies of oil and gas, fuel and equipment for the first nuclear power plant, as well as maintenance of military aviation, composed of Soviet MIG 29 and SU 25. Moreover, given the scheduled November Presidential elections (2016) Bulgarian politicians did not want to lose the 'Russian vote', as many Bulgarians have traditionally positive attitudes towards Russia" (2017).

Turkey has not assumed any official position in the consultation process regarding the Romanian initiative ahead or after the Warsaw summit. Kogan of *European Security & Defence* journal explains briefly the Turkish position: "Turkey remains very reserved and cautious regarding its naval force participation. Yes, Turkey supports a limited and scaled-up NATO reinforcement of the Black Sea region but as long as it does not impact its interpretation of the Montreux Convention (2017, p. 14). In this sense, during a meeting of the heads of general staff of Balkan nations in Istanbul in May 2016, Turkish President Recep Tayyip Erdogan declared that he asked NATO Secretary General Jens Stoltenberg to deploy more assets to the Black Sea, otherwise this area becomes a Russian lake. Erdogan also mentioned that Turkey expects concrete results in this sense from the NATO summit in Warsaw (Sputnik International, 2016a). Turkey's cautiousness can also be explained by the numerous challenges this country faced both in terms of domestic and external affairs since the end of November 2015 up until the end of 2016. Indeed, it all started on 24 November 2015 when a Turkish combat aircraft shot down a Russian aircraft close to the Turkish-Syrian border in the context of the recent launch of the Russian military intervention in support of Syria's President Bashar al-Assad. Russia responded immediately through imposing sanctions on Turkey and conducting bombings in the disputed Syrian-Turkish border (Bertrand, 2015), meanwhile projecting its military power through more frequent warships sailing through Bosphorus as a way of 'enjoying the freedom of movement in peace time' under the provisions of the Montreux Convention (Pitel, 2016). The process of normalization of the Turkish-Russian relations started in June 2016 when Erdogan expressed his regret to Putin for the shooting down of the Russian aircraft. Only few days after the Warsaw summit, Erdogan was confronted with a failed *coup d'état* that deteriorated relations with the United States and strengthened those with Russia. Indeed, on 9 August 2016 Erdogan and Putin met in St. Petersburg for the first time since the incident of November 2015, being the first trip abroad of the Turkish president after the failed *coup d'état*. Even though the Turkish-Russian relations could have been deteriorated again by the assassination of the Russian ambassador to Turkey Andrei Karlov on 19 December 2016, Erdogan and Putin managed to mitigate the effects of this event and further

consolidated their countries' bilateral relations – their most-recent developments will be discussed below.

Ukraine welcomed the Romanian initiative ahead of the Warsaw summit. Indeed, Ukrainian President Petro Poroshenko declared in April 2016, during his visit to his Romanian counterpart, that "we support Romania's initiative to create a NATO-supported allied fleet. I emphasize that we're ready to join it after this initiative has been approved and supported by the Alliance. This is what has been agreed with Mr. President (Iohannis), and we are set to develop that cooperation" (cited in UNIAN, 2016). In this sense, an Allied enhanced naval cooperation could have helped directly this country by conducting actions assuring the freedom of navigation in the Black Sea, desperately needed by the Ukrainian vessels attempting to enter the EEZ around the Crimean Peninsula in the Black and Azov Seas. Subsequently, Ukraine had offered its Ochakiv Naval Base in Ukraine for the US-construction of a maritime center which was officialy launched on 25 July 2017 (*Sputnik International*, 2017a) and harmonised its national legislation on the admission of units of the armed forces of foreign states to the territory of the Ukrainian state in 2018 to participate in multinational exercises (Interfax-Ukraine News Agency, 2018).

Georgia has remained silent during the consultation process even though – as in the case of Ukraine – this country would definitely welcome an Allied enhanced naval cooperation assuring the freedom of navigation in the Black Sea. This necessity derives from the loss of the most of Georgian fleet during the 2008 conflict with Russia and is reflected especially in the case of its port Poti where the remaining Georgian Coast Guard vessels are facing the risk of being blocked to go beyond the coastal waters, on the basis of deterring a threat to the coast of Abkhazia, by the Russian fleet. According to some speculations such as the one promoted by the Russian analytical information agency *Vestnik Kavkaza*, Georgia has also been discouraged ahead of the Warsaw summit by its last minute forced withdrawal from the NATO's military exercise 'Anakonda 2016' hosted by Poland in June 2016 on the grounds of not escalating the tensions with Russia (Kalatozishvili, 2016) – hypothesis branded by Georgia's Minister of Defence as Russian propaganda meanwhile advancing medical reasons for the last-minute withdrawal of the Georgian Infantry Company (for details, see Ministry of Defence of Georgia – Press Statements, 2016). Subsequently, following in Ukraine's footsteps, Georgia offered NATO the possibility of using its national infrastructure for training purposes and even requested NATO to create a coast guard base in the port of Poti as part of NATO's efforts to boost security in the Black Sea region (Sputnik International, 2017b).

Overall, as it can be seen, it is worthwhile noting the difference of position of the stakeholders involved in the Romanian initiative. There are certain national interests and risk assessments that stopped the operationalisation of an Allied enhanced naval cooperation in the Black Sea so far. As Lucinescu remarked, the cooperation in the WBSR is affected by heterogeneity (politically, economically, culturally and religiously), lack of a culture of dialogue, military incidents, exacerbation of energy competition for existing resources and, furthermore, complicated due to the Kosovo precedent which feeds separatist and nationalist-extremist aspirations" (2011, p. 91). The division among the stakeholders of this initiative is definitely fuelled as well by Russia's actions in this sense – it could be seen in the dramatic shift of the Bulgarian position towards the Romanian proposal – as it serves its interests not to have neighbours united in a military development where Russia's access is denied by default. Indeed, some Russian military experts such as Konstantin Sivkov threatened that the creation of such a fleet would be a violation of the Montreux Convention and it can be regarded as an act of military aggression against Russia, with all the corresponding consequences (Sputnik International, 2016b).

The (post) Warsaw Summit effects on the Romanian initiative

The Warsaw summit of 2016 represented the turning point in the perception of NATO vis-à-vis the Black Sea riparian states (NATO, 2016).Within this summit the Black Sea's strategic importance was reiterated for the first time since the end of the Cold War while NATO signaled its anxiety regarding Russia's destabilizing activities in the region. However, as Joja & Manea remarked, "though in the aftermath of the Crimea annexation the Alliance promised to increase readiness in Europe and consolidate defense on the Eastern flank, the 2016 Warsaw focused only on the Baltic Sea. The differentiation between the Northern (Baltic Sea) and the Southern part (Black Sea) of the Eastern flank was conceptualised as 'enhanced' versus 'tailored' forward presence and translated into four battalions of Western combat troops on the ground and the continuous rotational presence in the North, while only training and staff units, no Western framework nations and intermittent rotational presence in the South" (2018). Even though Russia's recent destabilizing activities occurred in the Southern part of the Eastern flank, this imbalance in terms of resources allocated by NATO – favoring the Northern part of the Eastern flank – can be justified by the aforementioned lack of cohesion between the Black sea riparian states.

From another perspective, the Warsaw summit placed the Romanian initiative at a standstill rather than encompassing it under its authority – this status is maintained as of October 2018. Indeed, even though the 23rd paragraph of the Warsaw Summit Communiqué mentioned that "we [NATO] will continue to support, as appropriate, regional efforts by the Black Sea littoral states aimed at ensuring security and stability", the 41st paragraph acknowledged that "options for a strengthened NATO air and maritime presence will be assessed" (NATO, 2016). As Bugajski and Doran (2016, p. 4) pointed out "rather than committing itself to a naval buildup, NATO is more likely to support a semi-integrated structure for the navies of Romania, Bulgaria and Turkey, with funding for infrastructural modernization". This propension on NATO's behalf to empower the Black Sea states so as to ensure their own security through regional initiatives potentially enforced by NATO is not only about avoiding escalating tensions with Russia, but also about its historical institutional relations with Turkey in terms of using the latter's Straits. As Vladimir Socor noted, "long before the present crisis, Turkey was reluctant to accept NATO in its collective capacity to be present in the Black Sea. Instead, Turkey allowed warships of individual NATO member countries (the United States and others) to enter the Black Sea, more or less regularly, for port calls and joint exercises with riparian navies. For their part, NATO allies carefully complied with the limitations of the Montreux Convention (...) Turkey blocked NATO's proposals to allow Operation Active Endeavor (2001-2016), an Allied naval operation, to be extended from the Mediterranean into the Black Sea. Although NATO's proposals were compliant with the Montreux Convention, Turkey saw this operation as a collective one and blocked it, not least for that political reason. In August 2008, unilaterally interpreting the Montreux Convention, Turkey blocked the passage of an unarmed U.S. transport and hospital ship en route to Georgia during the Russian invasion of that country" (2016).

As of 2018, among the measures proposed since the Warsaw summit, the following have already been developed: the multinational brigade in Craiova, for which Romania is a framework nation, makes up the land component of the forward presence; in the air domain, some Allied states are voluntarily reinforcing Romania and Bulgaria's efforts for air policing; in the maritime domain, standing NATO maritime forces are present with more ships and more naval exercises (under the command of the Standing NATO Maritime Group 2 operating in the Mediterranean). A Black Sea functional centre, which focuses on the regional specific security issues and maintains tight links with the regional navies, has been established; last, but not least, a new enhanced training initiative aims to bring more coherence in all training

efforts (Anastasov, 2018). Not ultimately, NATO seems to reach a compromise in terms of the Southern part of the Eastern flank's requirement for reinforced security. By offering itself a wider space of maneuvering while temporize its decision on the operationalization of the Romanian initiative, NATO has recently committed to address the Russia's A2/AD in the Black Sea through its Readiness Initiative – *the Four Thirties*. In the preparation of the Brussels Summit of July 2018, NATO defence ministers held a meeting where they have set the military parameters of this development aimed to be operationalized by 2020 – 30 battalions, 30 air squadrons, and 30 naval combat vessels; all ready to use within 30 days – and its scope – to enhance the readiness of existing national forces and their ability to move within Europe and across the Atlantic (see NATO Public Diplomacy Division, 2018). All these (post) Warsaw developments have been indicated vaguely in the official communiqué following the most recent NATO summit organized in Brussels (11-12 July 2018), the 14th paragraph officialy acknowledging the launch of the NATO Readiness Initiative and its general parameters – as set during the NATO defence ministers' meeting of June – meanwhile the 26th paragraph mentioning though that "we [the Heads of State and Government participating in the summit] welcome progress towards the full implementation of the agreed measures, and particularly in the maritime domain, while noting that further work is required" (NATO, 2018). Based on this final remark, coupled with the opinion of some military experts such as Iulia Joja who argues in the light of the launch of NATO Readiness Initiative that members on NATO's Eastern flank would potentially still have to wait weeks for military aid in the event of Russian aggression (2018), the feasibility of the Romanian proposal for an enhanced naval cooperation in the Black Sea has not yet been decided by the NATO policymakers; as a consequence, its validation is still possible in the short-term.

The Montreux Convention – strategic and operational challenges for the Romanian initiative

Understanding the limits imposed by the Montreux Convention is highly-important for assessing the feasibility of the Romanian initiative. Having been signed in 1936 and updated unilaterally twice by Turkey only in terms of its provisions concerning the safety of navigation – in 1994 and 1998 –, Montreux Convention has legitimated ever since the Turkish control over the Bosphorus and Dardanelles Straits. This Convention sets the navigation rules through the Straits for both merchant vessels and warships in time of peace and in time of war (for full details regarding the provisions of the Montreux

Convention, see League of Nations, 1936). This paper analyses only the relevant provisions of the Montreux Convention for the Romanian initiative, namely those applicable to the warships in time of peace. In this sense, there are two perspectives that need to be taken into account.

Firstly, from an operational point of view, the Montreux Convention sets some restrictions depending on whether the warships belong to the Black Sea riparian states or not. Since the Romanian initiative is in full compliance with the Montreux Convention, both cases should be considered. On the one hand, as the Romanian initiative has been originally addressed to the riparian states, this convention imposed the following main restrictions on them: according to Articles 12 and 13, the submarines of these countries that are constructed, purchased or in need of being repaired outside the Black Sea are allowed to cross the Straits if they provide an eight-day notice in advance to Turkey and must travel by day, on the surface, pass singly and escorted by no more than two destroyers; even though the Convention contains no explicit prohibition on aircraft carriers, the maximum aggregate tonnage of 15.000 ton limit imposed to the foreign naval forces in course of transit through the Straits by Article 14 impedes the presence of the aircraft carriers in the Black Sea – as an exception, the Soviet Union developed its Kiev-class and Kuznetsov-class aircraft carriers as *aircraft carrying cruisers* and classified them as capital ships to comply with the Article 11 of the Montreux Convention that allows the Black Sea Powers to access the Straits with war vessels having a greater tonnage than the limit above mentioned (League of Nations, 1936, p. 221-223). The only war vessel of this type still possessed by Russia is the Admiral Kuznetsov aircraft carrying cruisers which at the end of October 2018 was highly-damaged by a crane which fell on to it while being overhauled at a floating dock near Murmansk (Rainsford, 2018). On the other hand, apart from some general limits applicable to all, the Montreux Convention sets the following main operational restrictions for the non-riparian states when sending war vessels in time of peace through the Straits: Article 13 – a notification given 15 days in advance to the Turkish Government; Article 14 – the total number and the maximum aggregate tonnage of all foreign naval forces which may be in course of passage through the Turkish Straits are limited to 9 and 15.000 tons, respectively; Article 18 – the maximum aggregate tonnage which non-riparian States may have in the Black Sea is 45.000 tons meanwhile the maximum aggregate tonnage of the vessels of war that one non-riparian State may have in the Black Sea is 30.000 tons. In addition, vessels of war belonging to non-Black Sea Powers cannot remain in the Black Sea more than 21 days (League of Nations, 1936, pp. 223-225). As a consequence, even though the Romanian initiative would be

operationalized, the current operational provisions of the Montreux Convention are permissive only to the riparian states; meanwhile the contribution of the non-Black Sea members of NATO would be limited in terms of quantity, quality and duration of their deployable capabilities in the Black Sea.

Secondly, as the enhanced naval cooperation has been originally announced by Romania to be also opened under NATO framework to the Black Sea members of the Eastern Partnership – Georgia and Ukraine – as well as for the non-Black Sea members of NATO such as the United States, understanding the application of the Montreux Convention in the Black Sea is very important from a strategic point of view as well. The current status quo undoubtedly favours Russia and Turkey and maintains as of now the two-hegemon paradigm in the Black Sea. It is worth mentioning that the US has never ratified the Montreux Convention even though this Great Power accepts in general terms its provisions. However, the recent increase of the American focus on the Black Sea suggests its desire to reconfigure the balance of power in the region by contesting the anachronic provisions of the Montreux Convention. Lucinescu indicates that in the following period we will witness an American attempt to promote a geopolitical revisionism in the Black Sea aimed to replace the preeminence of Russia and Turkey with a cooperative regional framework (2011, pp. 23-24). Indeed, the Romanian proposal for an Allied naval cooperation in the Black Sea can be regarded as an expression of this American ambition to contest the superiority of Russia and Turkey in the region. However, the operationalisation of the Romanian proposal in the near future depends on the evolution of the relations between Turkey and Russia on one side and between Turkey and the US on the other side. As mentioned earlier, the failed *coup d'état* of July 2016 attemped to overthrow the Erdogan regime deteriorated Turkey's relations with the United States and strengthened those with Russia. Adding insult to injury, Turkey's credibility as a NATO ally diminished severely ever since due to some controversial actions taken by the Erdogan regime after the failed *coup d'état*, such as: a massive purge of the officer corps educated in the West (Emmott, 2016; Jacinto, 2017); Turkey's intention to buy Russian S-400 defence systems (Al Jazeera, 2018); and a series of bilateral disputes with the US, including the extradition process of the Turkish cleric US-based Fetullah Gülen accused of orchestrating the failed *coup d'état*, the imprisonment on terrorism charges of the American evangelical pastor Andrew Brunson, diverging interests in Syria and Turkey's pressumed economic ties with North Korea. Indeed, the period August-October 2018 witnessed probably the lowest level of the US-Turkish relations, the Trump administration imposing – in an unprecedented decision for the US

to hit a NATO ally with sanctions – a two-row sanctions on Turkey, firstly based on the imprisonment of Andrew Brunson (BBC, 2018) and secondly based on illegal economic ties between a Turkish company and the North Korean regime (Harris, 2018). The US-Turkish tensions have recently shown signs of reaching a consensus as a result of the release of Andrew Brunson in the wake of Turkey's attempt to build an international case against Saudi Arabia over the murder of Saudi journalist Jamal Khashoggi in its Istanbul-based consulate, culminated with a bilateral meeting Erdogan-Trump in November 2018 in Paris during a dinner held by the French President Emmanuel Macron (Karabat, 2018).

Furthermore, as Toucas argued, "if it [Turkey] wants to remain a leading stakeholder in the region, Ankara will have to strengthen ties with Romania and Bulgaria (…) Only then, would Turkey be able to talk to Russia as an equal and positively use its peculiar relationship with Moscow as an asset to stabilize the region" (2018). Even though nowadays Turkey has some of its best relations with Russia, history proved that its national security can be highly-affected if found unprepared in assuring its own security. In other words, "there are no permanent friends or permanent enemies, only permanent interests" as revealed by an apocryphal aphorism considered by realists as a cornerstone of international relations. The Turkish Straits crisis is a relavant example in this sense with Turkey attempting to remain neutral during the Second World War, but forced under the pressure of the Soviet Union's request to allow Soviet shipping through the Straits and its subsequent show of naval force in the Straits, to call for US protection and subsequent NATO membership at the end of the WWII. A more recent case happened on 6 December 2015, amid tensions between Ankara and Moscow as a result of the November 2015 Russian Su-24 shootdown by Turkey, after footage emerged of a serviceman aboard Russia's Caesar Kunikov landing ship apparently aiming a surface-to-air missile launcher towards Turkey's largest city Istanbul while crossing Bosphorus (Hurriyet Daily News, 2015). As a consequence, these key arguments can favour the operationalization of the Romanian initiative in the near future.

Possible prospects for a permanent NATO Black Sea Fleet

The issue of a permanent NATO Black Sea Fleet can be easily resolved by revising the anachronic provisions of the Montreux Convention. However, apart from fearing direct retaliations from Moscow, Ankara is fully aware that, as Ogutcu put it, once Pandora's box is opened, you never know where it might end up – in addition, there is unwillingness among other parties, which had

signed the Convention to avoid any potential restrictions to free passage and incur the additional cost that may be brought on for ensuring the security of the waterways (2018). Therefore, the simplest method to increase the Allied naval presence in the Black Sea proves to be the most complicated one in the current international context. However, there are three major potential developments bypassing the Montreux Convention that would allow obtaining the ultimate presumed-goal of the Romanian proposal, namely the existence of a permanent NATO Black Sea Fleet or at least credible security guarantees for the NATO members of the Southern part of its Eastern flank.

First, the construction of the Kanal Istanbul, the man-made canal sought to be operationalised by Ankara in 2023 as a celebration of the centenary of the Turkish republic. The official argument for the construction of this infrastructure is to divert the critical volume of the maritime traffic from the Straits that have become some of the world's busiest choke points. Apart from being a measure directed to ensure the safety of navigation – indeed, the Straits are notorious for maritime accidents as over 140 occured since 2006 (Ogutcu, 2018) – the Kanal Istabul would allow the Turkish authorities to charge the shippers a transit fee for crossing it, a limited provision in this sense being available nowadays to Turkey when managing the Bosphorus and the Dardanelles Straits. Turkey has not adopted yet an official position regarding the inclusion of the Kanal Istanbul under the provision of the Montreux Convention; however, the Turkish Prime Minister Binali Yıldırım declared in January 2018 that Kanal Istanbul would not be subject to the Montreux Convention (cited in Franchineau, 2018). If that were the case, the deployment of naval assets in the Black Sea by NATO non-riparian states would be commited only to the jurisdiction imposed by Turkey and not to a binding international agreement as of now. However, even in the case Turkey decides to include the Kanal Istanbul under the provisions of the Montreux Convention, the revision of this Convention is compulsory as the signing parties are entitled to renegotiate its provisions taking into account this potential newly-emerged context. In any case, the operationalisation of the Kanal Istanbul forces Turkey to consult with all the other Black Sea riparian states as the Straits are the only maritime routes to the world's oceans available to them.

Second, an interesting proposal worth to be taken into account was launched by A. Cohen of *Atlantic Council* who argued in favour of reflagging some NATO naval assets under the three Black Sea members' flags in order to boost permanent Allied naval capabilities in the Black Sea (2016). Some scholars such as Bugajski and Doran sustained his proposal, adding though that NATO partner countries, particularly Ukraine and Georgia, need to be also

engaged in this process as they can offer harboring capabilities for NATO forces (2016, p. 16). Even though this initiative has not been so far officially assummed by NATO as it will be perceived undoubtedly as a provocation by Russia, some measures taken in this sense can be remarked. The most recent example is the case of the two U.S. Island-class patrol boats given, according to the Ukrainian media, to Ukraine on 27 September 2018 as free military aid from the United States (Ponomarenko, 2018).

Third, even without reinforcing its naval presence in the Black Sea with additional non-riparian states' combat vessels over the current limits imposed by the Montreux Convention, NATO can still offer credible security guarantees for its Black Sea members by creating a chain of A2/AD bubbles around the Russian bubble in Crimea. Esebua proposes the materialization of this initiative through the creation of a Black Sea Defense Coordination Center, an integrated network of all source data exchanged, and the combined capabilities of robust land-based mobile anti-ship missiles, mobile air defense systems, and sea and air surveillance radars, as well as aviation and naval assets (2017, p. V). Bugajski and Doran argue in favour of such an initiative given that a buildup of maritime capabilities is an expensive and long-term proposition meanwhile creating a robust A2/AD zone would entail lower costs for the Black Sea members of NATO than building a fleet of naval vessels (2016, p. 10). Not ultimately, according to Esebua this initiative can serve several goals such as: restriction of the freedom of action for Russia in the Black Sea; creation of robust individual defenses for littoral NATO member and partner states; enhanced regional cooperation and increased control of NATO over the region as whole (2017, p. 59).

Conclusion

Evolved as a reaction to the annexation of Crimea and its subsequent militarization by Russia, the Romanian proposal of 2016 for an enhanced naval cooperation in the Black Sea has not yet been decided by the NATO policymakers. The individual national interests and risk assessments of the Black Sea riparian states stopped its operationalisation for the time being even though the current status quo favours solely Russia and Turkey. As Celac et al. pointed out, "today, as during the Cold War, NATO's solidarity, its members' willingness to meet their defense obligations, U.S. leadership, and regional cooperation are key to this region's (WBSR) future peace and prosperity, and to all of Europe's" (2016, p. 20). On the one hand, the US is fully-aware of this equation – by recently increasing its political focus and military presence in the WBSR – and as a consequence, this region can witness

the emergence of an American-fuelled geopolitical revisionism aimed to replace the preeminence of Russia and Turkey with a cooperative regional framework such as the one proposed by Romania. Indeed, this potential development can resolve the current security requirements of this region still lacking credible security guarantees in the face of a potential Russian aggresion in spite of the recently-announced ones offered by the NATO Readiness Initiative. On the other hand, Turkey's recent volatile relations with the US and Russia impedes this country to ask for a revision of the anachronic provisions of the Montreux Convention that would allow an enhanced Allied naval presence in the Black Sea. However, the potential developments bypassing the Montreux Convention coupled with Turkey's determination to become a major actor in the region increase the odds for the operationalization of the Romanian proposal in the near future.

References:

1. Al Jazeera (2018) 'Erdogan: Turkey needs Russia's S-400 missile defence system', 31 August [online]. Available at: https://www.aljazeera.com/news/2018/08/erdogan-turkey-russia-400-missile-defence-system-180831103412006.html (Accessed: 25 September 2018).

2. Anastasov, P. (2018) 'The Black Sea region: a critical intersection', *NATO Review Magazine*, 25 May [online]. Available at: https://www.nato.int/docu/review/2018/Also-in-2018/the-black-sea-region-a-critical-intersection-nato-security/EN/index.htm (Accessed: 14 September 2018).

3. Barna, C. (2014) *România între prieteni şi duşmani, Decupaje geopolitice şi hărţi imagologice*. Bucharest: The Military Publishing House;

4. BBC News (2018) 'Andrew Brunson: US hits Turkey with sanctions over jailed pastor', 2 August [online]. Available at: https://www.bbc.com/news/world-us-canada-45036378 (Accessed: 25 September 2018).

5. Bertrand, N. (2015) 'Russia is already exacting its revenge on Turkey for downing a Russian warplane', *Business Insider*, 26 November [online]. Available at: https://www.businessinsider.com/russia-turkey-downed-jet-2015-11 (Accessed: 14 September 2018).

6. Blomfield, A. and Kirkup, J. (2008) 'Stay away, Vladimir Putin tells Nato', *The Telegraph*, 5 April [online]. Available at: https://www.telegraph.co.uk/news/worldnews/1584027/Stay-away-Vladimir-Putin-tells-Nato.html (Accessed: 2 September 2018).

7. Bozhilov, Y. (2017) 'The brief life of the idea for the creation of NATO black sea fleet', *New Europe*, 8 January [online]. Available at: https://www.neweurope.eu/article/brief-life-idea-creation-nato-black-sea-fleet/ (Accessed: 2 September 2018).

8. Browne, R. (2018) 'US show of force sends Russia a message in Black Sea', *CNN Politics*, 20 February [online]. Available at: https://edition.cnn.com/2018/02/19/politics/us-russia-black-sea-show-of-force/index.html (Accessed: 6 September 2018).

9. Bugajski, J. and Doran, P. (2016) *Black Sea Defended - NATO Responses to Russia's Black Sea Offensive*, Strategic Report No. 2. Washington: Center for European Policy Analysis.

10. Bulgarian News Agency, (2016) 'President Plevneliev: Bulgaria Is Well Aware of Risks Stemming from Disrupted Balance in Black Sea Region', 9 July [online]. Available at: http://www.bta.bg/en/c/DF/id/1374043 (Accessed: 12 September 2018).

11. Celac, S. et al. (2016) *Why the Black Sea matters*, Bucharest: New Strategy Center.

12. Cohen, A. (2016) 'NATO Should Stand Up Black Sea Command Before It's Too Late', *The Atlantic Council*, 5 July [online]. Available at: http://www.atlanticcouncil.org/blogs/new-atlanticist/nato-should-stand-up-black-sea-command-before-it-s-too-late (Accessed: 22 September 2018).

13. Commission of the European Communities. (2003) *Wider Europe – Neighbourhood: A New Framework for Relations with our Eastern and Southern Neighbours* [online]. Available at: http://eeas.europa.eu/archives/docs/enp/pdf/pdf/com03_104_en.pdf (Accessed: 3 September 2018).

14. Daly, J. (2014) 'Hot Issue: After Crimea: The Future of the Black Sea Fleet', *The Jamestown Foundation*, 22 May [online]. Available at: https://jamestown.org/program/hot-issue-after-crimea-the-future-of-the-black-sea-fleet/ (Accessed: 9 September 2018).

15. Emmott, R. (2016) 'Exclusive: Turkey purges NATO military envoys after failed coup', *Reuters*, 12 October [online]. Available at: https://www.reuters.com/article/us-turkey-nato-exclusive/exclusive-turkey-purges-nato-military-envoys-after-failed-coup-idUSKCN12C16Q (Accessed: 15 September 2018).

16. Emmott, R. (2017) 'NATO to launch Black Sea force as latest counter to Russia', *Reuters*, 9 October [online]. Available at: https://www.reuters.com/article/russia-nato/nato-to-launch-black-sea-force-as-latest-counter-to-russia-idUSL8N1MK150 (Accessed: 3 September 2018).

17. Esebua, K. (2017) *Russian build-up on the Black Sea and recommendations for U.S.-NATO counter-strategy*, Thesis, Monterey: Naval Postgraduate School.

18. European Parliament Press Releases. (2015) *Russia is no longer a strategic partner of the EU, say MEPs* [online]. Available at: http://www.europarl.europa.eu/news/en/press-room/20150604IPR62878/russia-is-no-longer-a-strategic-partner-of-the-eu-say-meps (Accessed: 5 September 2018).

19. Figes, O. (2014) 'Putin needs to show more restraint than hero to avoid a new Crimean war', *The Guardian (International edition)*, 28 February [online]. Available at: https://www.theguardian.com/world/2014/feb/28/putin-restraint-crimea-war-ukraine-russia-nicholas (Accessed: 7 September 2018).

20. Franchineau, H. (2018) 'How Istanbul's man-made canal project could trigger an arms race in the Black Sea – and why China is watching closely', *The South China Morning Post*, 3 June [online]. Available at: https://www.scmp.com/news/world/europe/article/2149025/how-istanbuls-man-made-canal-project-could-trigger-arms-race-black (Accessed: 15 October 2018).

21. Freire, M. R. (2017) 'War in Ukraine and European and European Security: Reset, Reverse or Revoke?' in Sadik, G. (ed.) *Europe's Hybrid Threats*. Newcastle: Cambridge Scholars Publishing, pp. 11-28.

22. Fukuyama, F. (1992) *The End of History and the Last Man*. New York: Free Press.

23. Harding, L. (2008) 'Bush backs Ukraine and Georgia for Nato membership', *The Guardian (International edition)*, 1 April [online]. Available at: https://www.theguardian.com/world/2008/apr/01/nato.georgia (Accessed: 2 September 2018).

24. Harris, G. (2018) 'U.S. Imposes Sanctions on Turkish Company for Trade With North Korea', *The New York Times*, 4 October [online]. Available at: https://www.nytimes.com/2018/10/04/world/asia/us-sanctions-turkey-north-korea.html (Accessed: 5 October 2018).

25. Hurriyet Daily News (2015) 'Turkey not planning to revise Montreux Convention on Bosphorus rights', 8 December [online]. Available at: http://www.hurriyetdailynews.com/turkey-not-planning-to-revise-montreux-convention- on-bosphorus-rights-92226 (Accessed: 2 October 2018).

26. Interfax-Ukraine News Agency (2018) 'Poroshenko signs law allowing foreign troops into Ukraine for drills in 2018', 29 January [online]. Available at: https://en.interfax.com.ua/news/general/480694.html (Accessed: 18 September 2018).

27. Jacinto, L. (2017) 'Turkey's Post-Coup Purge and Erdogan's Private Army', *Foreign Policy*, 13 July [online]. Available at: https://foreignpolicy.com/2017/07/13/turkeys-post-coup-purge-and-erdogans-private-army-sadat-perincek-gulen/ (Accessed: 15 September 2018).

28. Jankowski, D. (2018) 'Six Ways NATO Can Address the Russian Challenge', *The Atlantic Council*, 4 July [online]. Available at: http://www.atlanticcouncil.org/blogs/new-atlanticist/six-ways-nato-can-address-the-russian-challenge (Accessed: 15 September 2018).

29. Joja, I. (2018) 'Dealing with the Russian lake next door: Romania and Black Sea security', *War on the rocks*, 15 august [online]. Available at: https://warontherocks.com/2018/08/dealing-with-the-russian-lake-next-door-romania-and-black-sea-security/ (Accessed: 5 September 2018).

30. Joja, I. and Manea, O. (2018) '2018 NATO Summit: Finally a focus on the Black Sea?', *Real Clear Defense*, 11 July [online]. Available at: https://www.realcleardefense.com/articles/2018/07/11/2018_nato_summit_finally_a_focus_on_the_black_sea_113596.html (Accessed: 8 September 2018).

31. Kabanenko, I. (2017) 'The Kerch Strait Bridge: A New Threat to Regional Stability', *Eurasia Daily Monitor*, 14(106) [online]. Available at: https://jamestown.

org/program/the-kerch-strait-bridge-a-new-threat-to-regional-stability/ (Accessed: 12 September 2018).

32. Kalatozishvili, G. (2016) 'Georgia is symbolically on NATO's side in Black Sea', *Vestnik Kavkaza*, 20 June [online]. Available at: http://vestnikkavkaza.net/articles/Georgia-is-symbolically-on-NATO-s-side-in-Black-Sea.html (Accessed: 15 September 2018).

33. Karabat, A. (2018) 'Will meeting of Erdogan and Trump in Paris mend US-Turkish ties?' *Middle East Eye*, 8 November [online]. Available at: https://www.middleeasteye.net/news/US-Turkey-Relations-383472060 (Accessed: 9 November 2018).

34. Kogan, E. (2017) 'Are Russia and NATO on the Collision Course around the Black Sea Region?', *European Security & Defence*, vol. 5, pp. 14-15.

35. Kortunov, A. (2018) 'One More Time on Greater Europe and Greater Eurasia', *The Russian Council*, 2 October [online]. Available at: http://russiancouncil.ru/en/analytics-and-comments/analytics/one-more-time-on-greater-europe-and-greater-eurasia/?sphrase_id=18968492 (Accessed: 3 October 2018).

36. Kramer, A. E. (2008) 'NATO Ships in Black Sea Raise Alarms in Russia', *The New York Times*, 27 August [online]. Available at: https://www.nytimes.com/2008/08/28/world/europe/28russia.html (Accessed: 3 September 2018).

37. League of Nations (1936) 'Convention regarding the Rdgime of the Straits, with Annexes and Protocol. Signed at Montreux, July 2oth, 1936', *Treaty Series*, vol CLXXHI, No. 4001-4032, pp. 213-241.

38. Lucinescu, I. C. (2011) *Rolul României în asigurarea securității în Regiunea Extinsă a Mării Negre*. Bucharest: ANIMV Publishing House.

39. Lucinescu, I. C. (2016) 'The North Atlantic alliance and the security challenges in the Wider Black Sea Region. Present and Future', *The 11th International Scientific Conference - Defense Resources Management in the 21st century*, Brasov.

40. Mearsheimer, J. (2001) *The Tragedy of Great Power Politics*. New York: W.W. Norton & Company.

41. Ministry of Defence of Georgia – Press Statements. (2016) *Statement of Minister of Defence of Georgia with regard to "ANAKONDA-16"* [online]. Available at: https://mod.gov.ge/en/news/read/5060/minsitris-gancxadeba-anakonda-2016-dakavshirebit (Accessed: 15 September 2018).

42. Ministry of Temporarily Occupied Territories and IDPs of Ukraine - Press Releases. (2018) *Deployment of Russian S-400 Missile Systems "Triumf" in Crimea Is a Threat not only for Ukraine, but for the Entire Black Sea Region*. [online]. Available at: http://mtot.gov.ua/rozgortannya-rf-raketnyh-kompleksiv-s-400-triumf-v-krymu-zagroza-ne-tilky-dlya-ukrayiny-a-j-dlya-vsogo-chornomorskogo-regionu/ (Accessed: 12 September 2018).

43. NATO. (2008) Bucharest Summit Declaration – 03.04.2008 [online]. Available at: https://www.nato.int/cps/ua/natohq/official_texts_8443.htm (Accessed: 2 September 2018).

44. NATO. (2016) Warsaw Summit Communique - 09.07.2016 [online]. Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (Accessed: 3 September 2018).

45. NATO. (2018) Brussels Summit Declaration - 11.07.2018 [online]. Available at: https://www.nato.int/cps/ic/natohq/official_texts_156624.htm (Accessed: 3 September 2018);

46. NATO Public Diplomacy Division. (2018) *NATO Readiness Initiative*, Press & Media Section [online]. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_1806-NATO-Readiness-Initiative_en.pdf (Accessed: 19 September 2018).

47. Novinite–Sofia News Agency (2016) 'Gazprom Puts Forward New South Stream Route', 28 April [online]. Available at: https://www.novinite.com/articles/174250/Gazprom+Puts+Forward+New+South+Stream+Route (Accessed: 18 September 2018).

48. Ogutcu, M. (2018) 'Revising the Montreux Convention', Hurriyet Daily News, 12 April, [online]. Available at: http://www.hurriyetdailynews.com/opinion/mehmet-ogutcu/revising-the-montreux-convention-130148 (Accessed: 12 October 2018).

49. Olszanski, T.A., Sarna A. and Wierzbowska-Miazga, A. (2014), 'The consequences of the annexation of Crimea', *OSW*, 19 March [online]. Available at: https://www.osw.waw.pl/en/publikacje/analyses/2014-03-19/consequences-annexation-crimea (Accessed: 8 September 2018).

50. OstroV, (2016) 'The DNR is actively working to develop its own navy – Tymchuk', 29 February, [online]. Available at: https://www.ostro.info/news/529/ (Accessed: 15 September 2018).

51. Pantazi, C. (2016) 'România vrea o brigadă multinațională NATO pe teritoriul său', *Hotnews*, 4 April, [online]. Available at: https://www.hotnews.ro/stiri-esential-20913195-exclusiv-romania-vrea-brigada-multinationala-nato-teritoriul-sau-mihnea-motoc-ministrul-apararii-anunta-noi-achizitii-pentru-armata-transportoare-blindate-corvete-inca-escadrila-avioane-f16-interviu-v.htm (Accessed: 2 September 2018).

52. Pitel, L. (2016) 'Russian warships and naval assets sailing through Bosphorus strait has Turkey frightened', *The Independent*, 6 March, [online]. Available at: https://www.independent.co.uk/news/world/europe/russian-warships-and-naval-assets-sailing-through-bosphorus-strait-has-turkey-frightened-a6914796.html (Accessed: 15 September 2018).

53. Ponomarenko, I. (2018) 'Ukraine accepts two US patrol boats after 4 years of bureaucratic blockades', *The Kyiv Post*, 27 September, [online]. Available at: https://www.kyivpost.com/ukraine-politics/ukraine-accepts-two-us-patrol-boats-after-four-years-of-bureaucratic-blockades.html (Accessed: 5 November 2018);

54. Popa, A. V. (2018) 'The Twofold Outcome of Russia's Hybrid Warfare in Ukraine', *Governance, Intelligence & Security*, Cluj, submitted.

55. President of Romania – Press statements. (2016) Declarația de presă comună a Președintelui României, domnul Klaus Iohannis, cu Președintele Republicii

Bulgaria, domnul Rosen Plevneliev – 15 June, [online]. Available at: http://www.presidency.ro/ro/media/politica-externa/declaratie-de-presa-comuna-cu-presedintele-republicii-bulgaria-domnul-rosen-plevneliev (Accessed: 12 September 2018).

56. Rainsford, S. (2018) 'Russian aircraft carrier Admiral Kuznetsov damaged by crane', *BBC News*, 30 October, [online]. Available at: https://www.bbc.com/news/world-europe-46030113 (Accessed: 31 October 2018).

57. Renz, B. and Smith, H. (2016) 'What does Russia want? The importance of understanding Russian goals and intentions' in Renz, B. and Smith, H. (eds.) *Russia and hybrid warfare – going beyond the labe*l. Helsinki: Kikimora Publications, pp. 14-21.

58. Reuters, (2016) 'Bulgaria says will not join any NATO Black Sea fleet after Russian warning', 16 June [online]. Available at: https://www.reuters.com/article/nato-bulgaria-blacksea/bulgaria-says-will-not-join-any-nato-black-sea-fleet-after-russian-warning-idUSL8N19835X (Accessed: 12 September 2018).

59. Scheipers, S. (2016) 'Winning Wars without Battles: Hybrid Warfare and Other 'Indirect' Approaches in the History of Strategic Thought' in Renz, B. and Smith, H. (eds.) *Russia and hybrid warfare – going beyond the label*. Helsinki: Kikimora Publications, pp. 47-51.

60. Socor, V. (2018) 'NATO Summit Puts Black Sea Strategy on Hold for Another Year (Part Two)', *Eurasia Daily Monitor*, 15(118) [online]. Available at: https://jamestown.org/program/nato-summit-puts-black-sea-strategy-on-hold-for-another-year-part-two/ (Accessed: 10 September 2018).

61. Sputnik International, (2016a) 'Erdogan Criticizes NATO Over Low Military Activity in Black Sea', 11 May [online]. Available at: https://sputniknews.com/world/201605111039422760-erdogan-nato-black-sea/ (Accessed: 13 September 2018).

62. Sputnik International, (2016b) 'Why NATO's Growing Presence in Black Sea Won't Change the Strategic Balance', 1 June [online]. Available at: https://sputniknews.com/military/201606011040598984-nato-black-sea-russia-strategic-balance-analysis/ (Accessed: 16 September 2018).

63. Sputnik International, (2017a) 'US Starts Building 'Maritime Operations Center' in Ukraine, Here's Why', 13 August [online]. Available at: https://sputniknews.com/military/201708131056425592-us-ukraine-maritime-facility/ (Accessed: 2 October 2018).

64. Sputnik International, (2017b) 'Georgia Proposes Clever Way to Cheat Montreux Convention, Host NATO in Black Sea', 2 March [online]. Available at: https://sputniknews.com/politics/201703021051210603-georgian-nato-black-sea-coast-guard-proposal/ (Accessed: 2 October 2018).

65. Sputnik International, (2018) 'Turkstream, Nord Stream 2 Vital for EU to Meet Growing Gas Demand – Gazprom', 3 October [online]. Available at: https://sputniknews.com/europe/201810031068541255-nord-stream-2-gas-growing-demand/ (Accessed: 16 September 2018).

66. The Kremlin. (2014) *Address by President of the Russian Federation* – 18.03.2014 [online]. Available at: http://en.kremlin.ru/events/president/news/20603 (Accessed: 4 September 2018).

67. The Kremlin. (2015) *Russian National Security Strategy* [online]. Available at: http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf (Accessed: 4 September 2018).

68. The Presidential Administration – Romania. (2015) *National Defense Strategy 2015-2019*, [online]. Available at: http://www.presidency.ro/files/userfiles/National_Defense_Strategy_2015_-_2019.pdf (Accessed: 4 September 2018).

69. Toucas, B. (2017) 'The Geostrategic Importance of the Black Sea Region: A Brief History', *Center for Strategic & International Studies*, 2 February [online]. Available at: https://www.csis.org/analysis/geostrategic-importance-black-sea-region-brief-history (Accessed: 6 September 2018).

70. Toucas, B. (2018) 'Turkey Has No Allies in the Black Sea, Only Interests', *Center for Strategic & International Studies*, 13 February [online]. Available at: https://www.csis.org/analysis/turkey-has-no-allies-black-sea-only-interests (Accessed: 25 September 2018).

71. Urcosta, R. B. (2017) 'Ukraine Struggles to Retain Presence in Azov Sea With Plans for New Canal Around Crimea', *Eurasia Daily Monitor*, 14(128) [online]. Available at: https://jamestown.org/program/ukraine-struggles-retain-presence-azov-sea-plans-new-canal-around-crimea/ (Accessed: 15 September 2018).

72. UNIAN Information Agency, (2016) 'Poroshenko: Ukraine happy to join 'allied fleet' in Black Sea if created', 21 April [online]. Available at: https://www.unian.info/politics/1326318-poroshenko-ukraine-happy-to-join-allied-fleet-in-black-sea-if-created.html (Accessed: 12 September 2018).

73. UNIAN Information Agency, (2018) 'Russia amasses 32,000 troops, Iskander and S400 systems in Crimea – Ukraine', 24 April [online]. Available at: https://www.unian.info/politics/10093373-russia-amasses-32-000-troops-iskander-and-s400-systems-in-crimea-ukraine.html (Accessed: 10 September 2018).

74. Wade, J, (2017) 'Russia's A2/AD in Crimea', *Conflict Observer*, 7 July [online]. Available at: http://conflictobserver.com/russias-a2ad-crimea/ (Accessed: 10 September 2018).

75. Yuhas, A. and Jalabi, R. (2014), 'Ukraine crisis: why Russia sees Crimea as its naval stronghold', *The Guardian (International edition),* 7 March [online]. Available at: https://www.theguardian.com/world/2014/mar/07/ukraine-russia-crimea-naval-base tatars-explainer (Accessed: 7 September 2018).

COORDINATION OF COUNTERACTION TO TURMOIL IN THE ECONOMIC SPACE OF THE BLACK SEA REGION

Tetiana IEFYMENKO*

Abstract

The article highlights the directions of strengthening territorial economic security in the Black Sea region. Taking into account the strategic role of this region in the development of sustainable and secure partnership, the author suggests focusing on shaping the future, regarding the principle of coordinated scenarios and actions of the member-states to the Organization of the Black Sea Economic Cooperation.

The article stresses that for the countries of the region the geopolitical significance of regional challenges is largely due to the jeopardized (enhancement, accelerated, impetus) dynamics of global and national risks, which fundamentally affect both the current state of affairs and subsequent forecasts. Therefore, cooperation in the joint development of strategic thinking, in forecasting and political planning should focus on allocating the funding and tools for transforming the Black Sea from the confrontation zone into a space for peaceful convergence of civilization values.

The author proves that common initiatives of sovereign governments should be oriented towards the protection of national interests. The effectiveness of the application of various methods of resolving military, political, economic and social problems will depend on the pace of institutional change at all levels. Consistent actions aimed at further detente in the region need to be coherent with the relatively low rates of global and national public perception of the need for new joint reforms aimed at realizing the goals of sustainable development in favour of global and regional players.

Keywords: *Economic security, sustainable development, Black Sea region, peaceful relations, national priorities.*

* Dr. Sc. (Economics), Professor, Academician of NAS of Ukraine, Honored Economist of Ukraine, SESE "Academy of Financial Management, Kyiv, Ukraine, efimenko@afu.kiev.ua (official).

Defining the problem in a general, its relationship with important scientific and practical tasks

In recent years, the global environment has seen a tendency for fundamental shifts. In particular, this refers to mutual uncompromising claims in the framework of long-standing contractual relations due to changes in the configurations of the established interests of actors at the global and regional levels, which necessitates decision making on the expediency of reviewing established in the 20th century agreements and treaties, political and economic unions, etc. On the one hand, the widespread internationalization of the activities of business entities really contributes to the formation of single markets for labor, goods and services, to the strengthening of the constructive linkage between real sectors of national economies, and further unification of the scope of financial transactions. However, on the other hand, unlike coordinated integration interaction, certain globalization processes are characterized by uncertainty and incompleteness. That is, although international barriers between countries are weakening, economic relations are developing in a one-sided and inconsistent way. At the same time, the next cycles of rethinking the format and content of the components of national competitiveness mostly coincide with transformations in the corridors of power.

The international and national security of the states located within the Black Sea and the Caspian Sea basins belongs to the geopolitical priorities of their strategic development agenda. The peculiarity of these territories is that throughout the entire history of human civilization ethnoses, cultures, trade and energy communications have been interlinked, connecting the European and Asian continents. Therefore, it is quite natural that the authorized persons of not only geographically close to the countries of the European Union, but also of those countries which have no direct access to the Black and Caspian Seas and are located at a considerable distance from them, are always involved in discussing the principal issues of further development of the region. (USA, China etc.)

Therefore, the professional community generally supports the IMF's view on the relevance of issues related to global integration trends (IMF, September 2017). The balance of economic and financial systems depends on creating a productive counteraction to the challenges of their imbalance in the periods of general and local recessions. It comes to the set of measures designed by governments and international organizations to address the challenges of the post-crisis recovery of national economies, signs of instability of all constituent parts of the international and public financial

space, increased inequality and differentiation of the social strata of the population as a result of migration processes, as well as the lack of quality jobs. Renewed development strategies in countries both with high, medium and low incomes should be able to resist spatio-temporal threats of crisis phenomena, including their geopolitical aspects.

Obviously, the above mentioned fully relate to the functioning of the Organization of the Black Sea Economic Community (BSEC), which was set up in June 1992, which brings together 12 member states for the development of cooperation, peace and stability in the Black Sea basin. When defining future strategic priorities of each of them, it is necessary to bear in mind uncertainties of new probable upheavals – such as Brexit – the 2016 UK referendum on leaving the EU. It is also worth studying the prospects of the dissemination of macro trends of the so-called national egoism inherent in the modern state policy of the leading European and Asian countries, the United States of America, etc.

Analysis of the latest achievements and publications on this subject, which are based on the author

The works of such prominent scholars as J. Stiglitz, K. Reinhart and C. Rogoff, P. Krugman touch upon the issues of creating new instruments for managing and controlling processes of globalization on the methodological principles of institutionalist, system-managerial, technological approaches. Global imbalances bring about significant changes within established contracts and in the behaviour of economic agents. Famous American economists K. Freeman and F. Luke identified the situation in the field of research on socio-economic development issues on the eve of the financial and economic crisis of 2008-2009 as a collapse of consensus. In their view, the world needs to find common approaches to long-term changes in the future (Freeman and Louçã, May 16, 2002). Ukrainian researchers have repeatedly pointed out that global features cover economy, all areas of social activity, and also affect the sources, duration and degree of prevalence of failures in national economies, the balance of political and economic interests (Bilorus and Iefymenko, 2015, pp. 13-29). At the same time, according to the IMF expert community, the current wave of globalization cannot be considered unique (Tanzi, 2005), given the fact that in the past the intensity of resource flows of goods and capital also rapidly fluctuated. In addition, a relatively small part of the population of our planet is actually involved in the present transformation processes.

However, irreversible comprehensive changes at the level of strategies for stabilizing national economies of the leading powers show that the priorities are determined by the goals to ensure state and individual security in the global economic space, including their own levers of governance. Famous scientists as K. Waltz, H. Bull, R. Gilpint and others substantiate such approaches as "self-help international system" (Waltz, 2002, p. 134 and 1996).

This trend has become one of the main in the so-called Trumponomics – a new economic policy of President D. Trump. In the period up to 2022, it is expected that an increase in the US investment due to the weakening of fiscal pressure on business entities will enable the economy to revive. However, in the future, under conditions of uncertainty, a set of measures aimed at realizing purely national interests needs to be adjusted to maintain the positive dynamics of volume macroeconomic indicators. The reorientation of the US establishment from strategic positions of institutionalization of corporate globalism towards subordination of regional and national trade agreements to public policy of social justice was proclaimed in J. Fox' report (November 30, 2016). This document substantiates the main directions of the USA's updated strategy of competition in the world economy with a view to improve the living standards of the nation.

It is pointed out that the trade policy of the last quarter of the last century went bankrupt both economically and politically. In particular, the Report refers to the need for macroeconomic structural reforms, as well as to the need for adherence to the principle of acceleration of large-scale investments in education, skills upgrading and other characteristics of human capital assets, infrastructure and technological capital. Potential threats to the stability of sovereign social-economic systems (SES) while entering into interstate multilateral treaties for the benefit of large companies are shown in the sections of the Report on the risks of losers in politics against the background of bad economics.

Special attention should be paid to the application of standard approaches to the functioning of money as a standard of payment, accumulation and circulation, as well as measures of value and wealth nationally and globally. Therefore, it is no coincidence that the author's proposals for changing strategic national priorities place great emphasis on the need for regulatory restrictions on the manipulation of currencies of trading partners.

Identification of unresolved parts of the problem to which this article is devoted

For many centuries, regional security risks in the Black Sea region were caused by the factors associated with natural climatic conditions that are attractive to living. In addition, the competition between local and foreign economic agents historically grew to control the ways of traditional trade transit, which became the cause for internal or external military operations that periodically renewed. Long-term coexistence of various mixed national and ethnic groups on this territory, objective processes of mass migration of the population, etc. resulted in conflict situations over disputed boundaries of sovereign entities.

Currently, most democracies in the Black Sea region are actively developing their democratic processes. However, a number of factors are destructively influencing the attempts to disseminate the principles of democracy. This refers to the high influx of refugees, ethnic conflicts, which periodically bring about social unrest. An important element of the future stabilization in the Black Sea region should be the general agreement among the states, since almost all of the sovereign entities of the region face ethnic minorities' conflicts. Many experts point out that in their places of residence, the probability of further tension depends largely on policies conducted by the mother country. At the same time, the development of civil society is closely linked to institutional changes in the sate established order of interaction between citizens and authorities: from totalitarian or authoritarian to democratic partnership relations. For example, in the field of public finances of transitive states, the introduction of transparency and accountability are hampered by the inertia of formal and informal paternalistic rules in force in the Soviet and post-Soviet time. Entities operating in the shadow sector and the oligarchs may oppose social transformations, which slowdown legislation reforms, connected with more interactive participation of citizens in public administration.

In spite of significant regional differences, human capital in the Black Sea states is characterized by a high educational level. The scientific potential of many universities and research centres makes it possible to support research and innovations in a tough competitive environment due to rapid technological advances. However, market transformations in transitive economies due to international competition are accompanied by a significant growth of unemployment as well as by declining trends in the reproduction of labour – one of the main assets in the overall resource balance of the region.

Being employed abroad, citizens, working there on a temporary basis, contribute to the domestic economy, transferring money earned to their homeland. Emigrants with university certificates, having received permanent jobs and obtained the corresponding status at the place of residence, as a rule, replenish the Diaspora, as a result, investments in training skilled personnel are not paid off at the place of expenditure of budget funds. Thus, the decline in intellectual potential of labour force in many countries is becoming permanent. For example, in Bulgaria, Ukraine, etc., the outflow of able-bodied population occurs despite the fact that in the market conditions education, as well as the price level of the corresponding services, is adapted to the dynamics of supply and demand of skilled specialists. As a result, all of the above factors significantly constrain the pace of social changes in the spatio-temporal aspect.

Experts unanimously emphasize a number of problematic issues the countries of the region face, regardless of their level of development, their territory or economic structure[1]. In particular, this refers to the negative effects of certain demographic trends that are of a long-term nature. The cumulative variability of their content and scale varies widely in most countries. The threats they make to the quality and quantity of manpower, social security systems, and business environment can only be neutralized through structural reforms that affect the growth of competitiveness and resource productivity.

In conditions of insufficient resources, the quality and possibility of using production factors are restrained by external and internal risks of uncertainty, which are characteristic of globalization processes. Factors affecting the diffusion of innovations, when creating giant production and distribution chains, require from the supranational and state regulatory structures to ensure controllability of the degree of equality of business environment, common rules of access of economic agents to resources, avoidance of unfair stratification of producers and consumers by income, and compliance with environmental safety norms and social responsibility. Equally important is the observance of favourable working conditions and high standards of human rights.

---

[1] Harvard University, "Mihai Viteazul" National Intelligence Academy, Administrația Prezidențială. (2018). *SBSR. Security in the Black Sea Region. Shared Challenges, Sustainable Future Program*, Bucharest, May 28–31, 2018. Retrieved from http://www.sbsr.ro/wp-content/uploads/2018/06/SBSR-2018-Outcome.pdf/.

Formation of the goals of the article (task setting)

The aim of the article is to substantiate the directions of strengthening future economic safety of the BSEC countries, taking into account the obligations of each of them to regional treaties, in particular concerning the commonwealth of the Black Sea countries, European Union and others. In the global context, it is necessary to maintain a relevant level of socio-political and defence spheres as well as innovative development, invulnerability and independence of nations' interests regarding possible external and internal threats and influences. In the economic sphere, first of all, it comes to employment, solvency of parties to a contract etc.

Contents of the main study with full substantiation of the obtained scientific results

When formulating a regional policy in a globalized environment, the above arguments concerning fundamental changes in the US government policy, above all with regard to the protection of corporate interests in terms of preserving and creating more jobs, are undoubtedly worth noting. As J. Fox's report (Faux, November 30, 2006) showed, a large number of trade deals in the United States was accompanied by threats of reducing value added industrial chains, where operational activity required high professional skills. This situation occurred due to the fact that workers from countries that had free access to the US market initially agreed to a low wage. However, overtime they quickly acquired higher skills as they consistently developed their own training potential. Certain dangerous risks are associated with the probable reduction of business activity in the innovative industrial sectors, which depend on the interaction with production. As a result, stagnation trends were steadily spreading to research networks that generated new types of products. Due to similar situations in the high-tech industry of the USA a transformation of a positive trade balance into a deficit was observed. The threats further touched high-quality services, professional services (accounting, law, data analysis, internet management etc.). Indeed, in a deregulated global market, any professional activity associated with information technology can be localized in cheap labour countries.

Further BSEC economic security measures should be targeted at preventing the negative experience of radical changes in the United States

trade policy, which have become a major factor in deepening the gap between labour productivity of American workers and their incomes[2].

During the "cold war" on the territories adjacent to the Black Sea, autocratic and paternalistic principles dominated in the state systems of most coastal sovereign entities, and their economic systems developed on the principles of centralized planning. At the end of the 20th century the Black Sea region, for known geopolitical reasons, was virtually reoriented towards democratic reorganizations and transition to the market economy.

At the beginning of the 21st century countries of the region demonstrated a sustainable economic growth, against the tendencies of the EU enlargement, accompanied by an increase in domestic demand and export-import operations, in lending and direct foreign investments. The global financial crisis of 2008 caused serious imbalances, reduced output of goods and services. However, as in many other transit economies, in 2010s, signs of revival and further stabilization of national economies were demonstrated by almost all sovereign territorial entities.

Current geopolitical processes reflect the presence of tendencies of the so-called new reality, when the features of the hybrid nature are implemented both in different forms of confrontation and in the integration model of economic mechanisms of cooperation. According to V. Gorbulin, Academician of the National Academy of Sciences of Ukraine, World War I "(...) ended in the collapse of the German, Austro-Hungarian, Ottoman, and Russian empires. The second (WWII) ended in the collapse of British, French, Italian and Japanese ones. The Cold War remained on the world stage the only one truly acting superstructure - the United States." (Horbulin, 2018, June 15) The high level of current global antagonism is periodically turning into territorial armed conflicts. Noted "normalities" at the same time are characterized by events of chaotic destruction, which are the basis for the formation of new configurations of social relations in the external and internal environment of national development.

Consequences of the unprecedented confrontation between the leading global security guarantor – the USA – and China are trade and currency conflicts that, with high probability, can trigger a significant decline in the dynamics of the world economy. This opinion was made public by the head of the IMF, C. Lagarde (Statement, July 22, 2018), at a regular meeting of finance ministers and heads of central banks of the G20. Counteracting the growing risks due to increased tensions in the field of market commodity

[2]As the "EPI's Productivity-Pay Tracker" shows, the productivity has increased 6.6 times compared to 1973 (IMF, 2015, April).

exchange, as well as in the financial sector, should become measures that will help overcome contradictions in contractual relationships through international cooperation based on innovative partnerships avoiding emergency situations. At the same time, the role of the IMF as one of the centres of the global financial security system should remain unchanged.

According to J. Schumpeter, productivity growth is the result of the gradual development and discrete renewal of productive causal relationships and their components that inevitably leads to the creation of effective structures in the national economy. It is no coincidence that leading geopolitical leaders are constantly seeking consensus. This is evidenced by the results of a bilateral meeting of the US President D. Trump and Chairman of the European Commission J.-C. Juncker in Washington, July 2018. The parties have agreed to work on the abolition of already established contractual restrictions within the framework of the newly created working group. According to the parties' statement, the compromise has been reached due to the EU decision on the import of liquefied natural gas from the USA, as well as on the mutually beneficial growth of the supply of services, expansion of commodity exchange of chemical, pharmaceutical, medical products, etc.

According to the estimates of the IMF (April, 2018, p. 52), it is expected that the global growth in the group of emerging markets and developing economies is characterized by an improvement compared to similar data for the last quarter of 2017 (IMF, October, 2017, p. 14). The GDP growth will increase from 4.8% in 2017 to 4.9% in 2018 and to 5.1% in 2019, which is 0.1%. p. higher than in the previous survey, and then at the same level – in the medium term (IMF, April, 2018,p. 52). Economic growth in Europe with emerging markets and developing economies (excluding CIS countries)[3] is close to the

[3] According to the classification of countries used by the IMF, 51 countries belong to European countries. Among them: 27 * - with advanced economies, 12 ** - with emerging markets and developing economies, 12 *** - those that are CIS members (only 4 of them geographically belong to European countries). At the same time, Turkmenistan has changed its status as an associate member of the CIS since August 2005, Georgia has not been the member of the CIS since August 2009 and Ukraine - since April 2015, but according to the IMF classification they are included in this group of countries due to geographic location and similarity in the structure of economics (see: [IMF. (2018, April). Classification of countries: * Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Portugal, San Marino, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom of Great Britain and Northern Ireland; ** - Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Hungary, Kosovo, Macedonia, Montenegro, Poland, Romania, Serbia, as well as Turkey, although the vast majority of the territory and population of this country is situated in Asia; *** - Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Ukraine and Uzbekistan. (IMF, 2015, April)

world growth in its segment – 5.8% in 2017, 4.3% in 2018 and 3.7% in 2019 (IMF, April, 2018,p. 52). In the future, these parameters will remain in the same range due to the stabilization of the financial and economic space at the external level, as well as the increase in demand for goods and services in the euro zone. It should be noted that SBSR analysts emphasize the fact that among the countries of the Black Sea region, the forecast of the rise of the Turkish economy is slightly higher due to external demand and adequate policies of the government and the central bank in terms of providing state credit guarantees, forming expectations of participants in the financial market, ensuring the necessary level of monetization of the economy etc. (Table).

The overall economic growth of the CIS countries in the medium term will be 2.1-2.2% in 2017, reaching 2.2% in 2018, and then stabilize at about this level. According to experts from SBSR, in 2017, a powerful anti-crisis driver for the entire region was an increase in trade flows with counterparties in the CIS, as well as remittances from migrants from places of temporary employment to countries of permanent residence. Under the influence of the lower dynamics of the economy of the CIS countries when included in the IMF classification of this group of countries (with emerging markets and developing economies) to the total indicators for the European region in 2017 in 24 countries, the overall increase is estimated at 3.8%, in 2018 – 3.2, and in the medium term – 2.7-2.8% (see table).

Table: Indicators of economic dynamics of GDP
(Source: IMF, April, 2018)

Country/ group of country	**1991–2000**	**2001–2006**	**2007–2009**	**2010–2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**
	Fact						**Fact/estimation**		**Forecast**				
	GDP, real percent to the previous year												
BSEC Countries	**–1,0**	**6,3**	**1,7**	**3,9**	**1,6**	**0,2**	**1,2**	**3,5**	**2,9**	**2,6**	**2,5**	**2,4**	**2,5**
Azerbaijan	–2,6	16,3	15,1	2,7	2,7	0,6	–3,1*	0,1*	2,0	3,9	3,6	2,7	2,7
Albania	2,0	5,9	5,6	2,2	1,8	2,2	3,4*	3,9*	3,7	3,8	3,9	3,9	4,0
Bulgaria	–3,6	5,9	3,3	1,0	1,3	3,6	3,9*	3,6*	3,8	3,1	2,8	2,8	2,8
Armenia	2,9	12,7	2,2	4,3	3,6	3,3	0,3*	7,5*	3,4	3,5	3,5	3,7	4,0
Greece	2,5	4,2	-0,5	–6,3	0,7	–0,3	–0,2	1,4*	2,0	1,8	1,8	1,6	1,0
Georgia	5,3	7,7	3,8	5,8	4,6	2,9	2,8*	4,8*	4,5	4,8	5,0	5,2	5,2
Moldova	–5,7	6,7	1,6	5,6	4,8	-0,4	4,3*	4,0*	3,5	3,8	3,8	3,9	3,9
Russia	–2,1	6,5	2,0	3,8	0,7	–2,5	–0,2	1,5*	1,7	1,5	1,5	1,5	1,5
Romania	–1,4	6,1	3,1	1,0	3,1	4,0	4,8*	7,0*	5,1	3,5	3,1	3,1	3,1
Serbia	–2,2	6,0	2,7	0,9	-1,8	0,8	2,8*	1,8*	3,5	3,5	4,0	4,0	4,0
Turkey	3,8	5,3	0,4	8,2	5,2	6,1	3,2*	7,0*	4,4	4,0	3,6	3,6	3,6
Ukraine	–7,7	7,8	-1,6	1,5	-6,6	-9,8	2,4	2,5*	3,2	3,3	3,5	3,7	4,0
Emerging and Developing Europe, CIS	**–0,2**	**6,2**	**2,4**	**4,3**	**2,22**	**0,93**	**1,65**	**3,76**	**3,15**	**2,83**	**2,68**	**2,67**	**2,71**

* IMF estimates and preliminary data.

From the data in Table, we see that in the analyzed period (the fact for 1991-2018, the plan for 2018-2022) GDP dynamics of some BSEC countries differed from general trends for the organization.

In the period 1991-2017, which reflects the actual data, except for Ukraine (-7.7% in 1991-2000 and -1.6% in 2007-2008) Greece had minimum values in different years (+4 2% in 2001-2006 and -6,3% in 2010-2013). Maximum values in the period under review belong to Georgia (+ 5.3% in 1991-2000), and also Turkey (+ 8.2, +5.2, + 6.1% respectively in 2010-2013, 2014, 2015). In 2016 and 2017, the leaders were Romania (+ 4.8%) and Armenia (+ 7.5%). In Azerbaijan, fluctuations in the dynamics of the economy were observed from a minimum among the BSEC countries (-3.1% in 2016 and 0.1% in 2017) to a maximum (+ 16.3% in 2001-2006 and +15.1% in 2007-2009 years).

In the 2018-2022 planning period, more stable GDP dynamics is expected in the BSEC countries. This is evidenced by the forecast data, with all of them in the positive segment. In this period, the annual expected GDP growth in Ukraine is higher (3.2-4%) than the average for the BSEC. The leaders will also include Romania (+5.1% in 2018), Georgia (+4.8, +5.0% +5.2% respectively in 2019-2022), outsiders are Russian Federation (+1,5-1.7% in 2018-2022), as well as Greece (+1.0% in 2022).

In May (2018) during the SBSR event, international analysts once again emphasized that the main component of the economic structure in the Black Sea region is the real sector with a relatively low level of added value. At the same time, in Ukraine continues to dominate the heavy industry and agricultural production, while in other countries (Armenia, Moldova etc.), products of the agro sector. According to experts, the increase in the services sector and the rapid growth of the private sector are comparatively new trends in all Black Sea countries.

The security problems of the Black Sea region are mainly determined by the strategic importance of its role as one of the world's leading producers and suppliers of energy. Routes of energy supply flow through the territories of the states of the region, forming the so-called energy corridor between the Caspian Sea and the world markets. Moreover, the potential oil and gas reserves also make interest for many stakeholders. Therefore, there is no doubt that the export of natural energy resources and processing products will remain the traditional priorities for stimulating the growth of energy supply countries in the long-term period. Analytical data on comparing the annual real GDP growth of the BSEC countries (average weighted index of organization) to other countries is shown in Figure 1.

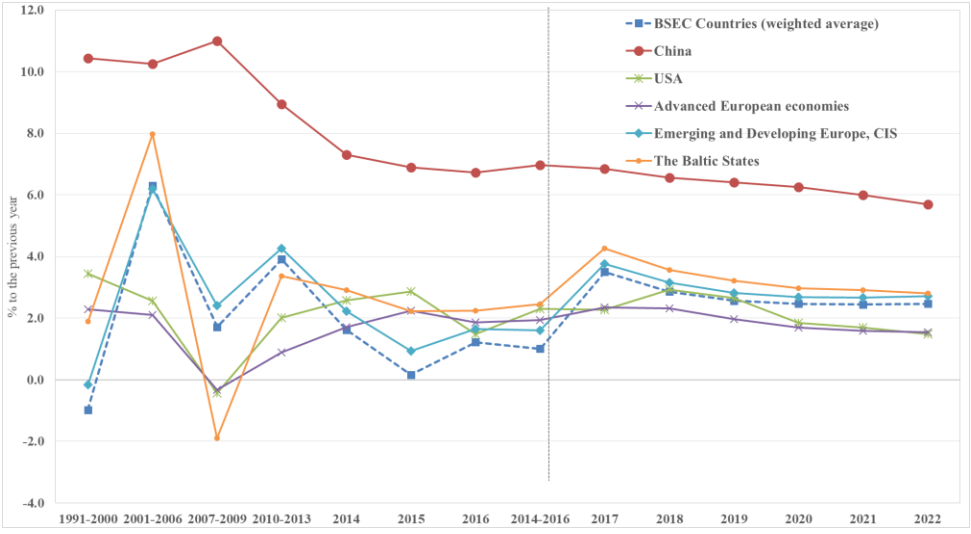


Figure 1: Indicator of real GDP growth, % to the previous year
(Source: IMF, 2018, April).

Trends shown in Fig. 1 indicate that in the analyzed period the fluctuations of the weighted average of GDP dynamics in the BSEC countries are close to the values of the GDP of the European countries with emerging markets and developing economies and the Baltic States. In the period of the institutional formation of 1991-2000, the GDP dynamics of the BSEC countries in the weighted average was lower than zero, although the Baltic States showed positive dynamics (+1.9%). For the advanced economies of European countries and the US, it is typical that a significant decrease of this indicator (below the zero mark - 0, 3% и -0,4% correspondently) was observed only in 2007-2009. During the same period, there was a decline in the Baltic countries (-1,9%). According to the forecast for 2018-2022, the rates of all the countries and their groups represented in Fig. 1 will be ranged from +1.5 to + 3.6%. China's economy grew steadily in 2001-2017, with a minimum increase of + 6.9% in 2017. The distinctive feature here is that during the crisis period of 2007-2009 its pace reached the maximum level (+ 11.0%). In the forecast period, the indicators of this country are also considerably higher relative to others (+5.7 – + 6.6%).

The analysis shows that the past disparities in the welfare of people in BSEC countries due to different demographic situation and the degree of

progress in economy were kept. However, in the future, humanity will be united by the goals of sustainable inclusive economic development. Their characteristic has been reflected in many international documents. The world community has come to the conclusion that the standard of living of a population depends not only on material revenues or the dynamics of GDP. The growth of welfare should take place with the provision of adequate education, health care, a comfortable ecological environment for the citizens of the country, as well as a guarantee from the state of personal security. Below is the actual and projected dynamics of GDP per capita, taking into account purchasing power parity (PPP), respectively, in 2014-2017 and 2018-2022 (Figure 2).

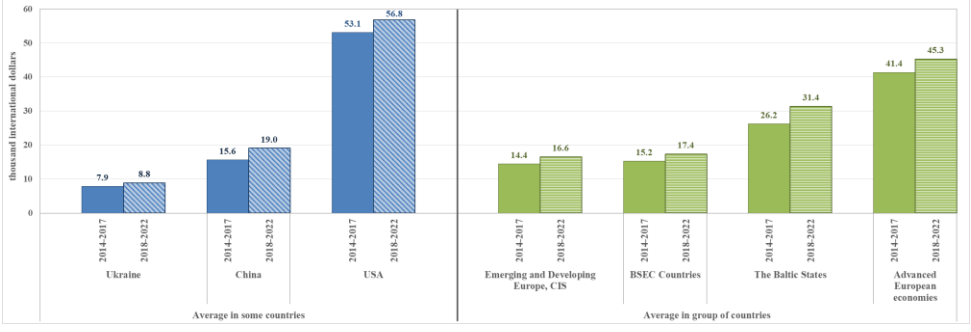


Figure 2: Average GDP per capita for PPPs in 2014-2017 and 2018-2020 (at constant prices), ths. international dollars (Source: IMF, 2018, April)

In BSEC, GDP per capita including PPPs is slightly higher than in other European countries with emerging markets and developing economies, but despite optimistic expectations, it will remain lower than in the countries of Europe with advanced economies, the Baltics, the USA and China. Due to the high rates of economic growth, this indicator in China for the first time outstripped its average value in the BSEC countries in 2014-2017 by 2.6%, but by 2022 such gap will increase to 9.2%, while 25 years ago the Chinese figure was lower in 4-5 times to the states of the Black Sea region. The minimum level of GDP per capita, taking into account PPP in the BSEC countries, was observed in Ukraine, Moldova, Armenia, Albania. By 2022, according to the forecast, the same figure will be less than 10 thousand international dollars in Ukraine and Moldova, its maximum value – in the range of 23-28 thousand international dollars – is expected in Turkey, Romania, Greece, Bulgaria.

The activities aimed at overcoming the lagging behind the BSEC countries from the world leaders and many European advanced economies is in the centre of attention of both government bodies and representatives of the professional community and business. Prospective plans for accelerating the development of countries should be made against the backdrop of reducing corruption, stopping the outflow of personnel, the need to achieve higher rates of growth of national economies, in order to eventually come to a category of developed countries. Figure 3 illustrates how the share of gross fixed capital accumulation for 1991-2016 changed.

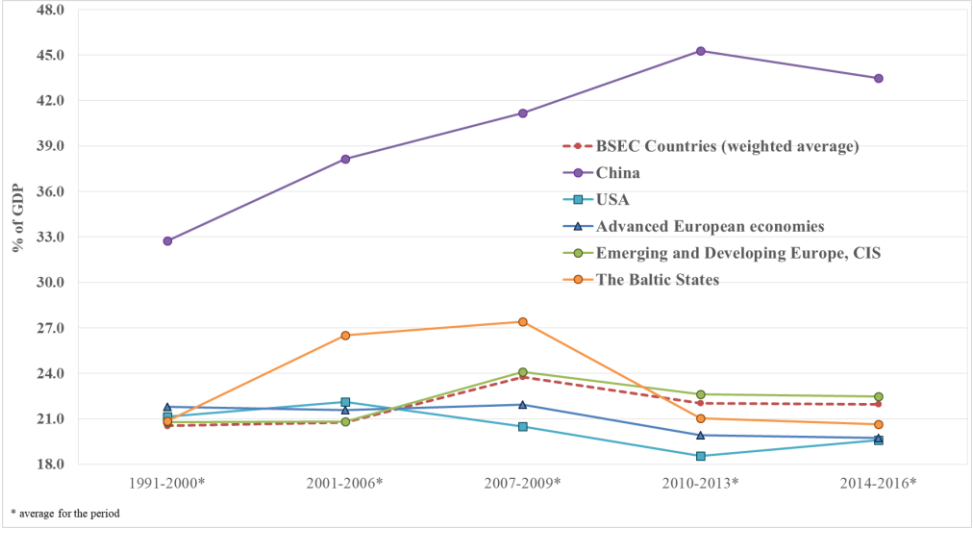


Figure 3: Indicator of the share of gross fixed capital accumulation for 1991-2016, % of GDP
(Source: UN. (n. d.). *DataCenter)*

Among the main tasks of structural reforms is the creation of conditions for the active involvement of domestic and foreign investments in production with high added value, with a target point for a significant increase in the share of gross fixed capital accumulation (GFCA) in GDP in the long-term period (not less than 25%). This means an increase in real investments by more than a third compared to their current volumes. It is impossible to develop dynamically and inclusive and expect stable growth in the long-term period if the share of final consumption in GDP reaches 85-90% (as is typical for the economies of Albania, Armenia, Greece, Georgia and Ukraine in 2009-2017). For example, in China,

since 1992, the share of GFCA in GDP has not decreased below 30%, and on average in 2014-2016 it was 43% for the corresponding share of final consumption 52%.

Despite the difficult situation, recent developments in BSEC countries show positive trends of institutional changes. In the near future, taking into account examples of the best world practice, it should be foreseen to make decisions on business simplification, privatization conditions that are more attractive to businessmen and favourable for the development of the economy, investment protection measures, and intellectual property rights.

In post-crisis periods, countries with developed partnership institutes (the US, euro zone) tended to stabilize the parameters of national economies rather than those where the creation of sustainable forms of socio-economic, interethnic equilibrium did not reach the level of confidence necessary to implement the general principles of interest of all stakeholders. Therefore, the leaders of BSEC countries should focus on the coordination of the public and private sectors of the economy, strengthening the principles of cooperation on the basis of public values, both in formal and informal business activities. Being balanced in the national legislation and coordinated at the supranational level, targeted interests will enable economic agents, regardless of ownership, to determine, in spite of political differences, the directions of economic prosperity and the ways of their implementation. In order to ensure the peaceful character of any changes, the political and socio-economic basis of the governmental bodies of all levels must be built in accordance with the principle of consensus of the views of society, business, and government. This approach implies that in the economic, military and other types of cooperation, the sovereign states of the BSEC should be guided by national priorities. The development of innovative mechanisms of cooperation between the state and business will help counteract the threats of post-crisis economic recovery in conditions of turmoil. It is well-understood that in the future intergovernmental and national forecasting of internal and external risks of the sustainability of SES is necessary.

Conclusions from the conducted research and prospects in this direction

Based on the research above, we can draw the following conclusions and recommendations on the designing of coordinated safe economic policy of the BSEC states.

1 Long-standing efforts of regional and global cooperation of stakeholders are hindered by old-established problems of tense relations, the manifestations of mutual unfriendliness between states; factors of uneven

political and socio-economic development of the countries of the Black Sea region are periodically amplified as well. However, under any circumstances, it is quite obvious that the problems should be solved in the framework of peaceful diplomatic relations provided that the strategic development goals and the ways to achieve them are clearly brought into line. Euroskepticism tendencies, Brexit UK initiative, clearly demonstrate the need for continuing structural institutional changes in the EU, which are also necessary to overcome crisis situations. Economic instability is still one of the reasons for declining competitiveness of individual countries in Europe, as well as for a prolonged recession in the euro area.

2 Modern development of the hybrid world order is accompanied by the restructuring of international, state and public institutions. The institutional framework for BSEC reform in all areas, both internal and external, should be based on a system of values, as well as a relatively stable political vector, along with a gradual increase in confidence and sustainability of the social-economic environment for global threats of a synergistic nature. Successful reforms will take place in case there is an economic development strategy and priorities such as the development of human capital, support for the domestic market, the environmentally balanced use of natural resources, renewal of infrastructure, the introduction of innovative investment projects aimed at fulfilling strategic development tasks. The choice of strategy depends on the consistency of legislative norms and informal restrictions such as cultural features and generally accepted traditions. In the process of reforming, either "shock" changes or evolutionary transformations may occur.

3 The enhanced modernization of economic policy will be more successful in the innovative initiatives of governments. The availability and effectiveness of the use of financial and other types of resources determine the successful achievement of the set goals. Debureaucratization of the economy, simplification of procedures and rationalization of existing restrictions for public expenditures aimed at infrastructure, support of private capital in foreign markets, in particular, in the political context, are fundamentally important. Designing of state targeted and budget programs should focus on certain priority areas and an effective medium-term budget process, which is implemented on a program basis.

4 Due to the organic interdependence and interconditioning of financial and economic sustainability factors, the strategic tasks of the BSEC countries at regional and national levels are: to avoid reproductive imbalances, desynchronization in the production and circulation of goods and money, as well as imbalances in the interests of economic agents and society. The movement of material and goods factors of production and their

monetary forms in real and virtual dimensions should be directed towards achieving the goals of sustainable development, improving the contradictions of the productive forces and production relations, liquidating material, monetary, informational and other manifestations of the inequality of economic agents throughout the world.

5 It is necessary to study the best practices of the EU countries in the common most effective anti-crisis strategies to achieve the sustainability goals of the developed SES. For example, in Germany and France, time has confirmed the validity of the postulate formulated by institutional theorists to enhance the role of the state: two components of a mixed system-the market and the state-are necessary for an efficient and humane society. Both these components are necessary for efficient functioning of the economy - it is impossible to clap with one hand (Samuelson, 1998). Developed countries are successful and competitive; the state there takes the initiative to create favourable conditions for sustainable business growth. To achieve such goals, all available tools are used, among which fiscal and monetary levers take one of the main places. Periods of advanced modernization of economic policy, as a rule, coincide with the triggering of innovations by state political will. However, due to the impact of signs of a new depressive wave in the leading states (euro zone, Brazil, India, China) on transitional countries, it is necessary to strengthen the resistance to instability at the regional level, to take coordinated measures to slow down post-crisis recovery. In the future, to speed up the approximation of the BSEC economies to the level of developed countries, governments should use a multidimensional set of coordinated tools and activities in innovation-investment, production, foreign economic and other spheres. Despite the signs of uncertainty on a global scale, it is worth strengthening macroeconomic, budgetary, monetary, and fiscal and currency tools in the state anti-crisis policy.

6 The growing volatility, the complications of global economic relations not only increases uncertainty, but also complicates the space in which decisions are made. Therefore, a clear understanding of the common ways of solving global problems seems necessary. In 2014, a fundamental report on global risks was presented in Davos. Experts came to the conclusion that the most dangerous in the next decade are economic threats in the form of financial crises, high unemployment and an increase in income inequality. At the same time, macroeconomic challenges remain the main ones for the global world. Among extremely significant risks with the most pessimistic results are: the budget crisis; unemployment; water crisis; income inequality; climate change; the collapse of information systems. In addition, for national economies, the most likely risks are: income inequality; extreme

meteorological conditions; unemployment; climate change; cyber attacks (*The Global Risks Report 2016*).

7 When developing the coordinated economic policy of the sovereign entities of the Black Sea region, one should take into account that the international community concentrates on the spread of interstate regulation of the processes of concentration and centralization of capital assets, the activities of multinational corporations and financial intermediaries. The need for coordination of international and national economic and political interests first of all calls for elimination of contradictions in the legislation of states, setting common goals for global development and developing universal mechanisms for their implementation. The ability of national governments and their managerial structures to provide swiftly for factors of ambiguity in the flow of real socio-economic processes increases the effectiveness of managerial decisions. Anti-crisis measures in each country should take into account national differences in fiscal, monetary and social policies, as well as the probable amount of stabilization resources of the real and financial sectors.

8 Technological ways of higher levels enrich mankind with universal information products; they make forecasting economic relations at the national and supranational levels possible due to the global logistics infrastructure. It is these circumstances that are the jam to fiscal reform, as well as compliance with restrictions on trade operations with the territories of tax havens aiming at rising of sovereign EU countries, where the efforts of all branches of power should be directed.

9 Any components of the economy, including the monetary sphere, should be aimed primarily at achieving public goals - improving the well-being both of individuals and the society (Stiglitz, 2016). With this, well-being of individuals will depend not only on the standard concepts of GDP, even with the inclusion of economic security. It is a much broader set of values, including coordination and social solidarity; trust in social, political, and democratic institutions. With imperfect regulation, financial systems can affect economic instability with protests and poverty, when, in response to crisis phenomena, the problems, inherent in the modern market economy, only worsen. The levers of the supranational currency should enhance the effectiveness of the economic space, political and social cohesion of the whole Europe. Therefore, the regulation of the euro as well as any national currency should be a means of achieving the goal, and not a goal in itself. Promoting the achievement of broader goals, including strengthening the foundations of a healthy nation, promoting core values are strategic principles of economic security. The

means cannot become a goal in itself in the absence of the organization of an integrated goal-setting, when uncontrolled ideologies and interests can contribute to the creation of economic structures that a few will benefit, but will jeopardize the interests of the greater part of the society.

References:

1. Bilorus, O. H., Iefymenko, T. I. (Ed.). (2015). *Financial globalization and European integration*: p. 13-29. Kyiv: SESE "The Academy of Financial Management".

2. Faux, J. (2016, November 30). U.S. *Trade Policy – Time to Start Over (Report)*. Retrieved from https://www.epi.org/publication/u-s-trade-policy-time-to-start-over/.

3. *Freeman, C., Louçã, F.* (2002, May 16). As Time Goes By: From the Industrial Revolutions to the Information Revolution. Oxford University Press.

4. Harvard University, "Mihai Viteazul" National Intelligence Academy, Administraţia Prezidenţială. (2018). *SBSR. Security in the Black Sea Region. Shared Challenges, Sustainable Future Program, Bucharest, May 28–31, 2018*. Retrieved from http://www.sbsr.ro/wp-content/uploads/2018/06/SBSR-2018-Outcome.pdf/.

5. Horbulin, V. (2018, June 15). Volcanic syndrome. *Dzerkalo Tyzhnia*. Retrieved from http://www.imf.org/en/News/Articles/2018/07/22/pr18302-argentina-statement-by-the-imf-managing-director-on-the-g20-meetings.

6. IMF. (2015, April). *World Economic Outlook Database*. Retrieved from http://www.imf.org/en/Publications/WEO/Issues/2016/12/31/Uneven-Growth-Short-and-Long-Term-Factors).

7. IMF. (2017, September). *Finance & Development Journal*. Retrieved from http://www.imf.org/external/pubs/ft/fandd/2017/09/pdf/fd0917.pdf.

8. IMF. (2017, October).World Economic Outlook. Seeking Sustainable Growth: Short-Term Recovery, Long-Term Challenges: p. 14. Retrieved from https://www.imf.org/en/Publications/WEO/Issues/2017/09/19/world-economic-outlook-october-2017.

9. IMF. (2018, April). World Economic Outlook. Cyclical Upswing, Structural Change: p. 52. Retrieved from http://www.imf.org/en/Publications/WEO/Issues/2018/03/20/world-economic-outlook-april-2018.

10. IMF Communications Department. (2018, July 22, 2018). Statement by the IMF's Managing Director on the G20 Finance Ministers and Central Bank Governors meeting in ArgentinaRetrieved from http://www.imf.org/en/News/Articles/2018/07/22/pr18302-argentina-statement-by-the-imf-managing-director-on-the-g20-meetings.

11. Samuelson P. Economics / P. Samuelson, W. Nordhaus. – 16th ed. – Boston, MA : Irwin/McGraw-Hill 1998. – 824 p.

12. Stiglitz J. E. The Euro. How common currency threatens the future of Europe / J. E. Stiglitz. - N. Y., 2016. - 416 p.

13. The Global Risks Report 2016 / World Economic Forum. – 11th Ed. [Електронний ресурс]. – Режим доступу: http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf.

14. Tanzi, V. (2005). *Social Protection in a Globalizing World*. Retrieved from http://www.rivistapoliticaeconomica.it/2005/mar-apr/Tanzi.pdf.

15. Waltz, K.(2002). *Theory of International Politics*: 134. Reading; Waltz, K. (1996). *International Politics is not Foreign Policy*. Security Studies: 2.

INTELLIGENCE, SECURITY AND INTERDISCIPLINARITY

INTELLIGENCE AND SOCIAL KNOWLEDGE A PHILOSOPHICAL INQUIRING ON THE SOCIAL EPISTEMOLOGICAL NATURE OF INTELLIGENCE AS A STATE INSTITUTION

Giangiuseppe PILI*

Motto: "*Nothing can be more in harmony with the nature of any thing than other individuals of the same species. And so (…) nothing helps a man to stay in existence and enjoy a rational life more than a man who is guided by reason. Also, the most excellent particular thing we know of is a man who is guided by reason; so our best way of showing what our skill and understanding are good for is by educating men so that at last they live under the sway of their own reason."*
Baruch Spinoza

Abstract

Intelligence is about speaking the truth to the policy-maker. However, this truth is not simply the result of an intellectual enquiring on something which is not in the eyes of the beholder. Intelligence is a social enterprise performed by a collective agent, namely the intelligence agency. Then, intelligence strives for the truth although this endeavor is a very difficult achievement indeed, so much so that intelligence is grounded on performing an entire intelligence cycle completed by an entire institution. Social epistemology is a new branch of analytic philosophy and it inquires the nature of social knowledge and collective agents. This paper considers the role of social knowledge inside intelligence as an institution of the state and it tries to address some fundamental questions related to the social epistemological nature of intelligence.

Keywords: *intelligence, social epistemology, theory, knowledge.*

* Ph.D. Philosophy and sciences of the mind, School of Law and Government – Dublin City University.

Introduction

It is always said that intelligence is about speaking the truth to the decision maker. However, this truth is not simply the result of an intellectual enquiring on something which is not in the eyes of the beholder. Indeed, intelligence deals with many different kinds of facts, such as natural facts (weather, environmental conditions, geography etc.) and social facts (states, institutions, organizations, armies etc.). Then, intelligence strives for the truth although this endeavor is a very difficult achievement indeed, so much so that intelligence is grounded on performing an entire intelligence cycle completed by an entire institution. The intelligence cycle is an entire epistemic activity based on gathering data and information, collecting them in order to analyze them to deliver a report whose goal is to enhance the rationality of a decision-maker. Then, intelligence is not an individual research agenda in which the analyst is the bookworm behind an esoteric piece of research. The analyst is just one social role to be performed by an individual, who is part of an institution whose main goal is the knowledge and foreknowledge of enemy's intentions, behavior and capability. Then, to reach this knowledge, the state needs an entire institution to perform this substantial and fundamental set of epistemic activities. The word "epistemic" here means that the main core function is deeply related to knowledge, although, of course, many other activities could be part of the process. However, if intelligence is about knowing the truths, then it is an *epistemic* activity. And as far as it is a collective enterprise, it is a *social* epistemic activity. Therefore, the intelligence outcome is the result of an institution that requests the coordination and activity of many people, as recognized by the scholars (Warner (2002), Ehrman (2009), Gill, Phythian (2012), Breakspear (2012),[1] Van Cleave (2013)). As it was stated by two prominent scholars, Mark Phythian and Peter Gill: "These all reflect the point that intelligence is a pre-eminently social and political phenomenon, not simply a technical discipline" Gill, Phythian (2016), p. 8. Then, intelligence is a collective group-activity formalized in a bureaucracy in order to let the intelligence officers work together for a common goal. The goal is defined by the policy-maker, who needs knowledge and information.

This paper is devolved to analyzing the social epistemological nature of intelligence. Jules Gaspard stated that "intelligence ultimately does not have just one essence, or none at all, but in fact it has more than one…" (Gaspard

[1] Breakspear considers intelligence as a "corporate capability to forecast change in time…". Therefore, he conceives intelligence as a social epistemic activity.

(2017), p. 558). If it is true, then one essence of intelligence is its social nature as it will be argued. In addition, intelligence today includes many different social epistemological institutions and activities, but this paper is focused only on intelligence as *state institution*. Although the following analysis can be easily applied also to the private sector, the focus here is to intelligence as state institution because it is still the most important of all. The paper is structured as follow: I will provide a philosophical analysis of intelligence as a fundamental social activity. Then, it will be considered what social epistemology is and why is so important for intelligence. In order to ground a social epistemological analysis of intelligence, it will be necessary to consider different aspects of its nature, from individuals to epistemic relevant organizations. Finally, an account of intelligence agencies as epistemic relevant institutions will be provided.

This paper tries to expand the discussion of a particular side of the intellingence theory. Other scholars developed theoretical perspectives (Marrin (2007), Warner (2009, 2017), Khan (2009), Gill (2010), Jackson (2010) Spadafora (2016), Galli (2016), Gaspard (2017), Phythian (2017), Marrin (2018)[2]). However, my approach is based on social epistemology and analytic philosophy, which is something still untried in the intelligence studies literature with some exceptions (Herbert (2006), Horn (2003), Bruce (2008), Rønn, Høffding (2013)). However, this would be one of the first attempt to develop a social epistemological understanding of intelligence as a state institution.

Intelligence is *inherently* a social activity – a philosophical proof

Before starting the social epistemological analysis, a general definition of intelligence would be useful:

> (I) Intelligence is a secret epistemic social process, carried out by a bureaucratic governmental society, which starts with a decision-maker's request and ends with knowledge and foreknowledge of enemy's intention and behavior to avoid surprises and to ground rational decisions.[3]

[2] This paper is particularly interesting as it is an update review of the state of the intelligence studies literature about the intelligence theory.
[3] I defended this definition in another work, Pili (forthcoming).

The definition conceives intelligence as a "secret epistemic social process", which will be the subset of intelligence which will be considered in detail below. The definition suggests that intelligence is indeed a collective group-work in which the main goal (knowledge and foreknowledge to be provided to the decision-maker) is provided by a team of different individuals, identified by their different role, mainly the intelligence gatherer, the intelligence analyst, the decision maker and the enemy. Then, a brief discussion of these distinctive roles is given to ground the argument. Is a decision-maker needed to intelligence? First, intelligence is knowledge and foreknowledge of the enemy's intentions, behavior and capabilities, and this knowledge is practically oriented, namely it is needed to take a rational decision. The decision has to be taken by an individual whose social role determines the responsibility to elaborate a rational choice. Then, the decision-maker is the individual who creates the need for intelligence. This means that intelligence without decision-maker is unthinkable. In a slogan, there is no intelligence without decision-makers. Then, intelligence is needed to enhance the effectiveness of power (Marrin (2007), p. 827, Warner (2009), p. 19, Gill, Phythian (2012), p. 19). However, the intelligence functions have to be performed by who have two epistemic duties: (a) to gather data and information and (b) to refine the information and deliver the product. These two core functions are performed by the intelligence gatherer and the intelligence analyst. Without the gatherer, the cycle of intelligence simply cannot start: intelligence process delivers an intelligence outcome selecting and refining information, which has to be gathered by somebody. However, gathering information and data is not enough, insofar it is a fundamental task of the intelligence process. Then, intelligence gathering has to be coupled with intelligence analysis. The two different functions must be performed by two different social roles, namely even though they can be done by the same *individual*, that individual is indeed entitle to have two different social roles with different duties and responsibilities (one thing is to gather information and data, another thing is to refine them to write a report understandable by a busy decision-maker). Then, ordinarily, the two intelligence functions are often (if not always) performed by different individuals with different social roles and related epistemic duties and responsibilities. Finally, the most counterintuitive of the four categories: the enemy. Many scholars agrees that enemy is essential to intelligence (Clausewitz (1832), Horn (2003), Treverton, Gabbard (2008), Luttwak (2009) Gill, Phythian (2012, 2016)). The main goal of intelligence is to discover enemy's intentions, capability and behavior.

"Intelligence is about nothing if not about 'out-thinking' the adversary". (Treverton, Gabbard (2008), p. 48). Eva Horn argued in favor of this position because enemy is an alive entity who always try to fight back. It would be interesting to discuss how enemy is defined, as far as it is a social construction of a social object that follows the rule of many other social objects. However, this would bring us too far from the main topic of this paper. Then, the social relation involved in intelligence could be expressed in this way:

R_{IV} (decision maker, intelligence gatherer, intelligence analyst, enemy) = Intelligence Social Roles

This is a quaternary relation among four different social roles and it shows that there are different relations among the related social roles:

R_1 (decision maker, intelligence gatherer)
R_2 (decision maker, intelligence analyst)
R_3 (decision maker, enemy)
R_4 (enemy, decision maker)
R_5 (enemy, intelligence analyst)
R_6 (intelligence analyst, decision maker)
Etc.

This list is provided to show that the social relations among the four different social roles are *not* symmetrical. In order to understand the relation between the decision-maker and the intelligence analyst, it is needed to see the same relation by both sides,[4] e.g. the decision maker comes before the intelligence analyst from a logical and temporary perspective: the decision maker has to put forward a request to the intelligence analyst to start the intelligence cycle.[5] Then, the combinations of these relations (R_1-R_6) show that

[4] This actually shows that
R (decision-maker, analyst) ≠ R (analyst, decision maker)
Where we can stipulate that the relation **!R** (decision-maker, analyst) is defined as follow:
!R = R (decision-maker, analyst) ∧ R (analyst, decision-maker)

Therefore, there are two different relations that bound the decision-maker and the analyst. This should be taken into the account when we analyze the relation between intelligence analysts and decision makers. Again, this means that the relation is composed by two different relations which are not symmetrical and that should be studied accordingly.

[5] Where $R_1 \neq R_5$ even if the relata are the same two social roles. This applies to all the couple of social roles presented in the list.

the intelligence is double bounded to both the enemy and the decision maker. Therefore, the complexity increases taking into the account the asymmetrical nature of that relations.[6] Now, I want to start with a brief introduction to social epistemology in order to go on the direction of a social epistemology of intelligence.

Social Epistemology – a brief introduction

Social epistemology is a relatively new branch of analytic epistemology. Its goal is to inquire knowledge, its role and its dynamics in social contexts. Since recent times, analytic epistemology was focused exclusively on individual epistemology, i.e. roughly, the study of how the cognitive subject knows something. Nevertheless, Alvin Goldman recognized that human knowledge cannot be understood only by one discipline: "epistemology should be a multidisciplinary affair" Goldman (1986), p. 1. Indeed, Goldman (1987) enlarged his interest on other sides of epistemology and he started a new way to think about knowledge in social contexts:

> My conception of social epistemology has some affinities with these disciplines [i.e. sociology, philosophy of science etc.], but the epistemological aim is not coterminous with theirs. These disciplines have strictly descriptive and explanatory goas, while the central aim of epistemology is normative, evaluative, or critical. (…) The epistemologist wishes to investigate epistemologically relevant properties of the mechanisms. What those epistemic proprieties are remains to be specified. Goldman (1987), p. 10.

Social epistemology is a normative discipline that evaluates the social practices involved in the production of knowledge in social domains. However, social epistemology is not interested only in the description of the social dynamics in which knowledge is involved. Social epistemology is not a sociological description of how a group of people forms knowledge in some specific social contexts (Goldman (1987, 1999, 2009, 2015)). In addition, it is not part of the philosophy of science, even if it considers some of the related problems (Goldman (2010)).

Social epistemology is divided in different subsets: (A) testimony and peer disagreement, (B) collective agents and their epistemology, (C) the analyses of institutions and systems (the taxonomy is based on Goldman-

[6] And it should increase furthermore if we consider that a relation that bounds three different entities is different by the simple sum of the relations that bound the entities per se.

Beddor (2015)). These areas can be furtherly divided. In the first categories, epistemologists study testimony and its capacity to justify beliefs (Code (2010), Goldman (2011), Millar (2011), Lackey (2011), Adler (2012), Goldman-Beddor (2015)); they study also how our beliefs, formed by the testimony of experts, are justified (Goldman (2011)). Finally, epistemologists consider also the problems of the peer disagreements (Sosa (2010), Kelly (2011)). Even if, historically, analytic philosophy is bounded on the assumption that knowledge is a matter of individual cognitive subjects, social ontology is a new branch of ontology (Bottazzi (2010), Mejers (2003), Searle (1990, 1995, 2007), Gilbert (1989), Bratman (2002)). Social epistemology considers under which conditions we can ascribe beliefs, justified beliefs and knowledge to social objects, e.g. collective agents such as institutions, organizations and societies (List and Pettit (2002), List (2011), Pettit (2011), Bird (2014)). Finally, some epistemologists consider specific aspects of institutions or organizations, which are important from an epistemological point of view (Goldman (1999, 2009, 2015), Anderson (2006), Talisse (2009), Fallis (2011), List (2011), Pettit (2011), Sunstein (2012)).

Social epistemology tries to understand how knowledge is formed and spread in social contexts. For this reason, epistemologists have different attitudes toward social epistemology: an individual based social epistemology, the epistemology of collective agents, and the specific analyses of particular domains. I do not want to go further in the description of the social epistemology but I want to say something more about its relevance for the intelligence studies.

First above all, intelligence is a social activity and, I think, it could be better analyzed by a social epistemological perspective much more than by an individual account of it. It would be impossible to exhaust its epistemological issues without a social epistemological analysis. Moreover, social epistemology should matter to the intelligence studies in many different ways: (a) intelligence analysts have to rely on other human beings to form their beliefs. It is impossible to have a good intelligence outcome without knowledge formed by testimony.[7] A specific analysis about testimony under secrecy should be of invaluable significance. This kind of analysis would be

[7] Human Intelligence is entirely based on the relationship between two different subjects. Open source intelligence is grounded on the open sources, which are basically video, audio and texts, i.e. testimony of facts reported through different ways of communication.

very interesting from a philosophical perspective as well. In fact, I did not find any useful philosophical analysis of secrecy within the epistemological theories. As stated by Stephen Marrin: "Finally, while there are efforts to develop intelligence theories related to intelligence analysis and produce-consumer relations, there are ideas being explored by other disciplines which could be considered intelligence theory" (Marrin (2018), p. 486). I think social epistemology could be one of these disciplines. (b) I will try to consider an analysis about the intelligence institutions. In fact, I think that the analysis of the epistemological practices of social objects is particularly fruitful to intelligence studies. (c) A detailed rational reconstruction (description) of intelligence organizations would be extremely useful for social epistemological accounts applied to systems and for the intelligence studies as such. Finally, (d) there are social epistemological accounts that deals directly with the evaluation of precise social systems whose goal is to provide knowledge. Don Fallis analyses Wikipedia and the Encyclopedia Britannica from an epistemological perspective in order to assess their relative and absolute epistemic efficiency (Fallis (2011)). I think that similar analyses could be useful for the epistemology of intelligence as well. This kind of studies would request some intelligence experts, interested in social epistemology. A social epistemological analysis of intelligence would be a great step toward an epistemology of intelligence.

A social epistemological account of institutions

Individuals, social relations and societies: Now I want focus my attention to the intelligence agencies and their nature. CIA, KGB, GCHQ, AISE, STASI are examples of intelligence agencies. Intelligence agencies are organizations: they are groups of individuals bounded by social relations. These groups have epistemic relevant goals to be reached according to their mission. In fact, different intelligence agencies can have multiple aims and some of them are not necessarily 'epistemic goals' (e.g. covert actions). An epistemic goal can be defined as a question or a problem that can be solved by the formulation of a set of propositions, formed by a reliable cognitive process. Although the intelligence agencies have many objectives, they are constitutionally grounded on their epistemic goals defined by their mission as the scholars point out.

In order to understand the nature of an intelligence agency as a social object, it is requested to distinguish different kinds of social objects and social subjects, e.g. society, organizations, institutions, and epistemic relevant

institutions. Let us start from the simplest social object. A society is *at least* a set of individuals. In fact, a set of individuals not bounded some social relations can be intended as a 'society'. For example, a random group of American people is still a kind of society. Nevertheless, this is not the case of an institution, because the social relations that bound the members are complex and not fixed by chance. Therefore, an institution is a particular kind of society. First, social relations bound the members of an institution: there is an interaction among the individuals part of an institution. Let us suppose for a moment that this is not the case. The members of an institutions simply cannot work together without the stipulation of social relations among them. They would not be organized as a group. They can just work together in the sense that they act alone even if they are grouped in some ways (for example, they stay in the same buildings). Therefore, these relations have to be 'social'. They have specific features that characterize them: they are not generic relations. For example, *a* and *b* are in spatial relations such that *a* is on the left of *b* and *b* is at north respect on *a*: these relations are not essential to characterize the social bounds among the members of an institutions. Therefore, an institution is a society in which all social relations bound the behavior and the beliefs of *all* the members of that organization. Of course, other kinds of relations appear (spatial relations, time relations and so on), but they are *not* essential to the definition of the nature of an institution as such. Therefore, an institution requests a set of social relations that bound the behavior and beliefs of the members of a particular institution.

Societies and Organizations: An institution is not only a set of people related together by social relations, e.g. a chess club. An institution is an *ordered* set of individuals, i.e. the social relations among the individuals shape a formal structure, whose shape depends on the institution's goals and rules. An intelligence agency, a football team, the public transport system, a university, an army are organizations with a different formal structure. In fact, their formal structures vary because of their different goals. This does not mean that organizations or institutions with similar or identical goals have necessarily the same structure. The point here is just that the goal of an organization shapes its structure and different kinds of organizations and institutions have different structures because of their different aims. Let us consider a possible characterization of an organization:

> (Org) An organization *O* is an ordered set of individuals $i_1 \ldots i_n$, related through social relations $R_1 \ldots R_n$, in order to reach a declared common goal *g* such that the formal structure of *O* depends on *g*.

As we proved before, the social relations among the members of an organization have to be of a particular kind. They are not as such by chance. They have to be defined by a strictly formal procedure that should be endorsed by the organization itself. Therefore, an organization is an ordered set of individuals whose structure is defined by a set of rules endorsed by the organization itself in order to reach a declared goal. This set of rules constitute the essence of the organization and it could be conceived as its 'constitution'. Every organization has a 'constitution', which is an explicit and defined set of rules, expressed in the natural language (Searle (1995), Bottazzi (2010)). John Searle considered this point:

> (…) institutional facts exist only within systems of constitutive rules. The systems of rules create the possibility of facts of this type; and specific instances of institutional facts such as the fact that I won at chess or the fact that Clinton is president are created by the application of specific rules (…). It is perhaps important to emphasize that I am discussing *rules* and not *conventions*. It is a rule of chess that we win the game by checkmating the king. It is a *convention* of chess that the king is larger than a pawn. "Convention" implies arbitrariness, but constitutive rules in general are not in that sense arbitrary. Searle (1995), p. 28, italics in the text.

Thus, an organization *O* exists if and only if (a) the order of the set of individuals is defined by its constitution, expressed in natural language and (b) the set of relations among the members of the organization is defined by the organization itself. In fact, two individuals i_1 and i_2 part of *O* have two roles R_1 and R_2 and these roles shape their relations between them within *O*. An agency's chief has a different relation with his inferior than his inferior with a peer. These differences are not simply owed to a spontaneously self-organization of the people. On the contrary, they are fixed in advance by the constitution of the organization. The *quality* of the relations can vary but not the *nature* of the relations.

The definition of the social roles within an organization requests a particular function. Searle (1995) calls it 'status function'. Before recalling it, I

want to quote another passage, which is useful to sketch the notion of 'function' involved in this context:

> 1. Whenever the function of *X* is to *Y*, *X* and *Y* are parts or a *system* where the system is in part defined by *purposes, goals, and values generally*. This is why there are functions of policemen and professors but no function of humans as such – unless we think of humans as part of some larger system where their function is, e.g. to serve God.
>
> 2. Whenever the function of *X* is to *Y*, then *X* is *supposed to* cause or otherwise result in *Y*. This normative component in functions cannot be reduced to causation alone, to what in fact happens as a result of *X*, because *X* can have the function of *Y*-ing even in cases where *X* fails to bring about *Y* all or even most of the time. Thus the function of safety valves is to prevent explosions, and this is true even for valves that are so badly made that they in fact fail to prevent explosions, i.e. they *malfunction*. (Searle (1995), p. 19, italics in the text).

Thus, an organization has a constitution (i.e. a set of rules to define its goals and its structure) and the constitution formulates the function through which the organization defines the individuals' social roles. This function takes the general form: "*X* counts as *Y* or *X* counts as *Y* in context *C*" (Searle (1995), p. 28). Therefore, an intelligence analyst is not simply a cognitive subject. He is a cognitive subject part of an organization such that his specific role is defined by the organization through a function, allowed by the constitutional rules of that particular agency. This role is not an arbitrary concession of the organization but it is objectively recognized as such by all the members of that organization and by the state that founded that institution. In fact, all the members are obliged to follow the constitutive rules of their institution. I want to refine the (Org) definition:

> (Org[1]) *O* is an organization if and only if:
>
> (a) *O* is an ordered set of individuals $i_1 \ldots i_n$;
>
> (b) *O* has a constitution, i.e. a set of rules explicitly endorsed by *O* and expressed by a natural language;
>
> (c) the order of the set of individuals $i_1 \ldots i_n$ is defined by the constitution;

(d) the social relations $R_1 \ldots R_n$ are defined by the status function (defined by the constitution);

(e) O has a goal g, defined by the constitution, such that the formal structure of O depends on g.

The definition of specific organizations could be obtained by some restrictions on (Org^1): (a) we can discriminate the organizations by their members. In this case, two different organizations *A* and *B* can have the same structure, the same constitution, and the same goals but they can be different according to their members. For example, two different scientific committees can share the same goals and structure but the rules and the organization of the composition of the groups can vary accordingly. (b) We can discriminate two different organizations by their constitutions. In fact, different constitutions imply different organizations. (c) Two different organizations can be different for their goals, e.g. an NGO is different from a football team because they have different purposes.

Epistemic-relevant organizations: Now, I want to focus my attention on a particular kind of organization. If the primary goal of an organization is to form and spread knowledge, then, it is an epistemic-relevant organization. 'Epistemic relevance' means that the institution has an epistemic goal and it works only if it succeeds in delivering knowledge. The intelligence agencies are epistemic-relevant organizations. In fact, an intelligence agency has to provide knowledge and foreknowledge. Then, a general definition could be this one:

(ERO) An organization O is an epistemic-relevant one if and only if O is an organization whose primary goal g involves or requires knowledge to be reached.

(ERO) endorses the notion of organization, which is defined by (Org^1). Therefore, it is possible to considered a new detailed definition of an epistemic relevant organization, restricting the conditions expressed in (Org^1). However, I think the point is sufficiently clear.

Before turning our attention to institutions, I want to add that 'knowledge' can mean simply true belief in social epistemological contexts. According to Alvin Goldman:

One reason I focus on W[eak]-knowledge is to circumvent the intricate issues that surround the notion of S[trong]-knowledge. (…) A

> second and more important reason is that people's dominant epistemic goal, I think is to obtain true belief, plain and simple. They want to be *informed* (have true belief) rather than *misinformed* or *uninformed*. The usual rout to true belief, of course, is to obtain some kind of evidence that points to the true proposition and away from rivals. But the rationale for getting such evidence is to get true belief. Goldman (1999), p. 24.

In fact, an institution or an organization have an epistemic goal even if they do not want to find 'strong knowledge', i.e. at least justified true belief. For example, a comic review has an epistemic goal but it is not interested in a higher scientific endeavor. Thus, an epistemic goal is not necessarily to form 'strong knowledge' but something less, e.g. information, true belief. Of course, there are institutions and organizations that tries to form and to spread strong knowledge: a scientific magazine, a journal of philosophy, a paper of formal logic, and an intelligence analysis try to form and spread 'strong knowledge'. Therefore, an epistemic-relevant organization is committed to form weak *or* strong knowledge to reach its goals. An intelligence agency is an institution whose goal is to provide knowledge and foreknowledge of the enemy's intention and behavior to the decision maker. Therefore, the intelligence agency is an epistemic-relevant institution whose nature is set on the previous conditions.

Organizations, institutions and state institutions: An institution is a particular kind of organization. It can be an epistemic relevant organization or not. A state institution is a trustworthy organization part of a state, which is an institution itself. A state institution has a political goal, i.e. its goal is to allow the ordinary life of the state.

As I said before, we can operate some restrictions to (Org^1) in order to define some specific organizations. In this case, the best way to do it is to specify that (a) the 'constitution' of an institution is based on a political agreement set by the proxy of the state. (b) The goal of the institution is a political aim to be reached employing the state's resources. (c) In ordinary cases, the members of an institution are citizens of the state that founded that institution, or their right to be part of that institution was allowed by the state. Therefore, a definition of institution is given:

> (In) *I* is a state institution *S* if and only if:
> (a) *I* is an ordered set of individuals $i_1 \ldots i_n$, where $i_1 \ldots i_n$ are citizens of *S*;

(b) *I* has a constitution, i.e. a set of rules explicitly endorsed by *I* and expressed by a natural language, and this constitution is based on a political agreement;

(c) the order of the set of individuals is defined by the constitution;

(d) the social relations $R_1...R_n$ are defined by the status function (defined by the constitution);

(e) *I* has a goal *g*, defined by the constitution, such that the formal structure of *I* depends on *g* and *g* has a political value.

(In) is a detailed definition, provided by a set of restrictions on (Org^1). However, (In) is long and complex. Then, I want to add a different formulation:

(In^1) *In* is an institution of a state *S* if and only if *In* is an organization with a political goal, grounded on a political agreement fixed in a constitution, whose members are citizens of the state *S* in ordinary cases.

I think that (In) and (In^1) catch the same set of organizations. It is worthy to underline that an institution exists only within a state. In fact, an institution, as a state organization, is founded for a political goal and its resources are allowed by the state. Moreover, the members of an institution are citizens of a state. And even the people that are not part of that state, need some further documents or rights (given by the state) to be part of that state organization. Therefore, a state is requested to define who can be part of a certain institution and who cannot be part of it. The state founds an institution in order to defend its own existence, or secure or expand the ordinary life of the citizens. Then, the state allows the institutions to have the proper means to work. An intelligence agency is in fact an institution, it has a political goal and it is founded by a state, the state defines who can be part of an intelligence agency and it allocates the means and resources.

Intelligence agencies as institutions of the state: I want to move on in the social epistemological direction. Then, let us consider what an intelligence agency is. First above all, an intelligence agency is an epistemic relevant-organization.

An intelligence agency necessarily has to be as (ERO) prescribes. Let us suppose that this is not the case. It would turn to be an absurdum. In fact, according to the definition of intelligence provided before, intelligence is an epistemic social process that should "form knowledge and foreknowledge of

enemy's intentions". If we deny that an intelligence agency is an epistemic relevant organization, therefore we simply deny that it is capable to provide the intelligence outcome. Therefore, an intelligence agency has to be an epistemic relevant organization in order to deliver sound intelligence outcomes to the decision maker. Thus, an intelligence agency works when it respects (I) and (ERO). However, these conditions are not sufficient. An intelligence agency has to respect also (In) or (In^1) to work properly:

> (In^1) *In* is an institution of a state *S* if and only if *In* is an organization with a political goal, grounded on a political agreement fixed in a constitution, whose members are citizens of the state *S* in ordinary cases.

In fact, an intelligence agency is an institution of a state *S*, it has a political goal and its members are citizens of *S*. Is it possible to deny these conditions? Let us see why it is not the case. (a) An intelligence agency has to respect (I). The intelligence definition explicitly considers that an intelligence agency is a bureaucratic activity, and then it is part of the state. (b) The goal of an intelligence agency is fixed by a policy-maker. Therefore, an intelligence agency has a political aim. (c) If intelligence is a bureaucratic activity, therefore it has to be done by the citizens of a state. In conclusion, an intelligence agency can be defined in this way:

> (Int. Ag.) An institution *IA* is an intelligence agency if and only if it is an epistemic relevant state organization, whose political goal *g* is grounded on a political agreement fixed in a constitution, and the *IA*'s members are citizens of the state *S*, and *IA* provides intelligence in ordinary cases to reach *g* at time *t* both fixed by *S*.

I can give a detailed definition, such as (In). But I think that (Int. Ag.) is sufficient. The next step is to characterize some general features that an intelligence agency has to respect to work properly as an epistemic-relevant organization.

Intelligence agencies as epistemic relevant institutions

An intelligence agency has an epistemic duty to fulfill in order to reach its goals. The agency's goal shapes its own structure. An intelligence agency, as an epistemic-relevant organization, is capable to deliver knowledge and foreknowledge in ordinary circumstances. This is possible only if its members

fulfill their epistemic duties inside the agency: they have to solve problems that request their epistemic capabilities, e.g. information, beliefs, cognitive processes, communication etc. This epistemic activity is a social epistemic process carried out by the entire organization. The agency's members have also to cooperate to fulfill their goals *as members part of an organization*. Thus, the agency constitutive rules stipulate the members' social roles, which define their epistemic duties. In addition, coordination is requested in order to allow further refinements in the intelligence outcome throughout the entire intelligence process. Therefore, the intelligence outcome is the epistemic goal of the agency.

We can distinguish two different kinds of intelligence outcomes: (a) the single analyst's result and (b) the result of the institutional process. (b) implies (a) but not vice versa (the result of the institutional process is based on the result of the analysts' analyses). Therefore, the intelligence outcome is the result of a social epistemic practice in which the intelligence analyst's work is just a piece of it. The formal structure of an intelligence agency, as epistemic organization, is important for the final outline of the intelligence outcome. In order to show that the organization is much more important than its individuals are *per se*, I want to sketch a paradoxical case.

John and Jack are members of the same intelligence agency. John is the chief of Jack and Jack is an analyst. Jack has a source of information, Tom. John, Jack and Tom are part of an intelligence agency, which works in a strange way: John reports to the decision-makers information *I*, formed by wishful thinking. In fact, John never asks to Jack what Tom's knows. Jack speaks with Tom only if Jack feels to be lonely. Is this an intelligence agency? Let us suppose that this organization was founded by a state, Freedonia, and that John, Jack and Tom are citizens of Freedonia. Let us say that this agency was founded to warrant intelligence analyses to the Freedonia's policy-makers. This is a *bad* intelligence agency but after all, it is. Of course, it is not efficient and it is doubtful that it can provide an intelligence outcome at all. What is wrong with that intelligence agency? Why does it not work properly under the ordinary circumstances?

First of all, it doesn't work because the analysts do not do their job properly, at least from an individual epistemic perspective. In fact, John forms his beliefs through wishful thinking, and Jack does not ask anything relevant to Tom (etc.). Then, there is a problem in the ways in which the single analysts work. However, these are not the main problems. Even if John, Jack and Tom are epistemic virtuous cognitive subjects, it is questionable that the *structure* of the organization allows them to fulfil the agency's epistemic duty. Let us recall a problem considered before. An organization is not simply a society

whose members work in the same room. An organization is a collective subject in the sense that its shape is structured to fulfill a collective goal, which cannot be reached without some level of coordination. In fact, we can work together in the same room without any further relation. An intelligence agency works properly because its members are not put together randomly. An intelligence agency is an epistemic-relevant organization because its structure is *truth-conducive* with a good truth-ratio, e.g. it is reliable in providing their intelligence outcomes. The truth-conduciveness is a property of the cognitive process whose function is to form knowledge: "A truth-conducive or reliable process is sometimes described as a belief-forming process that produces either mostly true beliefs or a high ratio of true to false beliefs" (Becker (2009)).

The structural truth-conduciveness of an epistemic organization is an important feature of it. It means that if the members fulfill their epistemic duties correctly, and they convey the right outcomes to their colleagues, and this is allowed by the rules of the agency, then the structure of the organization allows a reliable result. If this organization is an epistemic-relevant institution, then it can form and spread knowledge to the policy-makers reaching its goal in ordinary circumstances. Therefore, the formal shape of the institution is fundamental to reach the goal fixed by the state and to maintain a sufficient quality of its result. Moreover, for the reasons we discussed before, it is impossible to have an (epistemically) reliable organization, whose structure is not truth-conducive. An intelligence agency works properly if and only if its formal structure is truth-conducive in ordinary circumstances. To sum up, an intelligence agency works properly if and only if:

> (a) The members of the agency fulfil their duties, fixed by their social roles, and, among them, the epistemic duties;[8]
>
> (b) The agency's formal structure is truth-conducive under ordinary circumstances (i.e. if (a) is met));
>
> (c) The members of the agency join a common and efficient coordination.

(a-c) are disjointed conditions, i.e. if (a) is not met, (b)&(c) could be met. Nevertheless, (a-c) should be met altogether to have a functioning intelligence agency. The independence of (a-c) is important because it shows

[8] I considered this point extensively in another place, Pili (forthcoming).

that an institution is much more complex that it appears. In fact, if its members fulfil their duties, but their social roles, fixed by institution's constitution, do not allow an efficient coordination, then the institution does not work correctly. However, an intelligence agency still resides on the quality of its analysts and members.

As Marrin put out, to be efficient an intelligence agency needs practitioners with a high sense of professionalization: "preventing corruption of the analytic product requires that intelligence analysts retain a strong sense of professional identity and integrity. (…) All that is required to prevent analytic politicization is a fair reading of the information available combined with integrity in its intepretation and honesty in its communication" (Marrin (2013), p. 54). But this is not sufficient for an intelligence agency to work. An intelligence agency works properly if all the members fulfil their epistemic duties, they are properly coordinated, and the agency's structure is truth-conducive. An agency cannot fulfil its goals without the ordinary fulfillment of the duties of its members. Therefore, an institution lives only if its members work properly.

Conclusions

The argument addressed two basic goals: to give a new theory of intelligence as "a function of government"[9] and to referencing it to the existing literature. By the way, I consider my attempt as a first step to be further refined. The social epistemology could enlighten more aspects of what I have considered now. I tried to show that intelligence is a social activity, which has an epistemic impact over the rest of the society. I analyzed the intelligence agency from a social ontological perspective in order to clarify some important feature of its nature. The philosophical investigation showed that an intelligence agency is an epistemic-relevant organization whose goal is to provide knowledge and foreknowledge of the enemy's intentions and behavior. The formal structure of the intelligence agency is definitely important. In fact, the intelligence agency works properly only if its structure is truth-conducive. In addition to that, the professionalization of the members is necessary in order to provide reliable intelligence outcome. Finally, I showed that the intelligence agency, as a state institution, has a political goal and it depends on the rules of the state.

[9] Marrin uses this expression. I preferred to frame the same concept in a different way but I think I am in the Marrin's line.

References:

1. Adler, Jonathan, (2015), "Epistemological Problems of Testimony", *The Stanford Encyclopedia of Philosophy* (Summer 2015 Edition), Edward N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/sum2015/entries/testimony-episprob/>.

2. Anderson E., (2006), "The Epistemology of Democracy", *Episteme*, Edimburg: Edimburg University Press, pp. 8-22.

3. Becker, Kelly, (2009), "Reliabilism". *The Internet Encyclopaedia of Philosophy*, https://www.iep.utm.edu/reliabil/

4. Betts, Richard, (1988), "Policy-makers and intelligence analysts: Love, hate or indifference?", Intelligence and National Security, NY: Routledge, 3:1, pp. 184-189.

5. Bird A., (2014), "When Is There a Group that Knows? Distributed Cognition, Scientific Knowledge, and the Social Epistemic Subject", in Lackey (ed.), *Essays in Collective Epistemology*, Oxford University Press, New York, pp. 42–63.

6. Bottazzi Emanuele, (2010), "Criteri Filosofici delle Organizzazioni Sociali", Torino, Tesi di dottorato.

7. Bratman, Michael, (1992), "Shared Cooperative Activity", *Philosophical Review*, voll. 101, N.2, pp. 327-341.

8. Breakspear, Alan; (2013), "A New Definition of Intelligence", *Intelligence and National Security*, 28:5, pp. 678-693.

9. Bruce, James, (2008), "Making analysis more reliable: Why epistemology matters to intelligence." In Geroge, Roger; Bruce, James (2008), Analyzing intelligence: Origins, obstacles, and innovations, Washington: Georgetown University Press,

10. Clausewitz, Carl V. (1832), *On War*, trans. Michael Howard and Peter Paret (1976), Princeton, NJ: Princeton University Press.

11. Code, L., (2010), "Testimony, Advocacy, Ignorance: Thinking Ecologically about Social Knowledge", in Haddock, Millar, Pritchard, (eds) (2010) *Social Epistemology*, Oxford: Oxford University Press.

12. Ehrman, J. (2009). What are We Talking About When We Talk about Counterintelligence? Studies in Intelligence, 53(2), 9.

13. Galli G., (2016), "Intelligence e scienze politiche", in Caligiuri M. (ed), (2016), Intelligence e scienze umane, Rubbettino, Soveria Mannelli.

14. Gaspard, Jules JS (2017), "Intelligence without Essence: Rejecting the Classical Theory of Definition." International Journal of Intelligence and CounterIntelligence 30.3 (2017): 557-582.

15. Gilbert, Margaret, (1989), *On Social Facts*, Princeton: Princeton University Press.

16. Gill, Peter, Phythian, Mark, (2016), "What Is Intelligence Studies?", The International Journal of Intelligence, Security, and Public Affairs, 18:1

17. Gill, Peter (2010), "Theories of Intelligence", in Johnson Loch (2010) (eds.), The Oxford Handbook of National Security Intelligence, Oxford: Oxford University Press, pp. 43-58.

18. Gill, Peter; Phythian, Mark; (2012), "Intelligence studies: some thoughts on the state of the art" in Annals of the University of Bucharest, 14, pp. 5-17.

19. Goldman, Alvin, (1986), *Epistemology and Cognition*, Harvard University Press, Cambridge.

20. Goldman, Alvin, (1987), "Foundations of Social Epistemics", in Synthese, Vol. 73 Issue 1, pp. 109-144.

21. Goldman, Alvin, (1999), Knowledge in a Social World, Oxford University Press, Oxford.

22. Goldman, Alvin, (2009) "Social Epistemology: Theory and Applications", Royal Institute of Philosophy Supplement, 64, pp. 1–18.

23. Goldman, Alvin, (2011), "A guide to Social Epistemology", in Alvin Goldman & Dennis Withcomb (eds.), Social Epistemology, Oxford University Press, Oxford, pp. 71-91.

24. Goldman, Alvin, (2012), "Social Epistemology", Stanford Encyclopedia of Philosophy, http://plato.stanford.edu/entries/epistemology-social/

25. Goldman, Alvin, (2014), "Social Process Reliabilism: Solving Justification Problems in Collective Epistemology", in J. Lackey, (ed.), Essays in Collective Epistemology, Oxford University Press, Oxford, pp. 11-41.

26. Herbert M., (2006), "The Intelligence Analyst as Epistemologist", International Journal of Intelligence and Counter Intelligence, 19:4, 666-684.

27. Horn, Eva, (2003), "Knowing the Enemy: The Epistemology of Secret Intelligence", Grey Room 11.

28. Hulnick, Arthur, S., (1986), "The Intelligence producer – policy consumer linkage: A theoretical approach", Intelligence and National Security, 1:2, pp. 212-233.

29. Jackson, Peter (2010), "On Uncertainty and The Limits of Intelligence", Johnson, Loch (2010) (eds.), The Oxford Handbook of National Security Intelligence, Oxford: Oxford University Press, pp. 452-471.

30. Kahn, David, (2001-2008), "An Historical Theory of Intelligence", Intelligence and National Security 16, 79-92 riedited in Gill, Marrin, Phythian (Eds.) (2009), Intelligence Theory - Key Question and Debate, NY: Routledge.

31. Kelly T., (2006), "The Epistemic Significance of Disagreement", Oxford Studies in Epistemology, Vol. 1, pp. 167-196.

32. Lackey, Jennifer, (2011), "Testimony Acquiring Knowledge from Others", in Alvin Goldman & Dennis Withcomb (eds.), Social Epistemology, Oxford University Press, Oxford, pp. 71-91.

33. List, Christian, and Pettit, Philip, (2011), *Group Agency*, Oxford University Press, Oxford.

34. List, Christian, (2011), "Group Knowledge and Group Rationality: a Judgment Aggregation perspective", in Alvin Goldman & Dennis Withcomb (eds.), Social Epistemology, Oxford University Press, Oxford, pp. 221-239.

35. List, Christian, and Pettit, Philip (2002), "Aggregating Sets of Judgments: An Impossibility Result", Synthese, 140, pp. 207–235.

36. Luttwak, Edward, (2009), "The grand strategy of the Byzantine Empire." Center for Strategic and International Studies in Washington 600. (2009).

37. Marrin, Stephen, (2001), "Intelligence analysis and decision-making: methodological challenges." Intelligence Theory. Routledge, 2001. 145-164.

38. Marrin, Stephen, (2007), "Intelligence Analysis: Structured Methods or Intuition?", American Intelligence Journal, pp. 7-16.

39. Marrin, Stephen, (2009), "Intelligece analysis and decision-making", in Marrin, Gill, Phythian (2009) (a cura di…) Intelligence theory: key questions and debates, Routledge, New York.

40. Marrin, Stephen, (2018), "Evaluating intelligence theories: current state of play", *Intelligence and National Security*, 33:4, 479-490.

41. Meijers A. (2003), "Can Collective Intentionality Be Individualized?", American Journal of Economics and Sociology, 62, pp. 167–183.

42. Millar A., (2011), "Knowing from being told", in Social Epistemology a cura di Alvin Goldman & Dennis Withcomb, Oxford University Press, Oxoford.

43. Pettit, Philip, (2011) "Group with Mind of Their Own", in Alvin Goldman & Dennis Withcomb (eds.), Social Epistemology, Oxford University Press, Oxford, pp. 242-267.

44. Phythian, Mark, (2017), "Intelligence analysis and social science methods: exploring the potential for and possible limits of mutual learning." *Intelligence and National Security* 32.5: 600-612.

45. Pili, Giangiuseppe, (forthcoming), "Toward a philosophical definition of intelligence".

46. Searle, John, (1990), "Collective Intentions and Actions", in Intentions in Communications, Mitt press, Cambridge (MA), pp. 401-416.

47. Searle, John, (1995), Construction of social reality, Simon & Schuster, New York.

48. Searle, John, (2007), "Social Ontology: the Problem and Steps Toward a Solution", in Intentional Acts and Institutional Facts, Springer, Dordrecth (NT), pp. 11-28.

49. Sosa, Ernest, (2010), "The epistemology of disagreement", in Haddock, Millar, Pritchard, Social Epistemology, Oxford University Press, Oxford.Spadafora G., (2016), "Intelligence e pedagogia", in Caligiuri M., (ed), (2016), Intelligence e scienze umane, Rubbettino, Soveria Mannelli.Treverton, Gregory; Gabbard, Brian, (2008), "Assessing the Tradecraft of Intelligence Analysis", Santa Monica: RAND.

50. Sunstein, Cass, (2012), "Deliberating Groups versus Prediction Markets", In Alvin Goldman & Dennis Withcomb (eds.), Social Epistemology, Oxford University Press, Oxford,, pp. 221-239.

51. Talisse, Robert, (2009), *Democracy and Moral Conflict*, Cambridge University Press, Cambridge.

52. Van Cleave, Michelle, (2013), "What is Counterintelligence? A Guide to Thinking and Teaching about CI", Intelligencer: Journal of U.S. Intelligence Studies, Vol. 53, N. 2.

53. Vivaldi, Alessandro, (2014), "Cultural Intelligence", Sicurezza Nazionale, Roma, https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/cultural-intelligence.html

54. Vrist Rønn, Kira; Høffding, Simon; (2013), "The Epistemic Status of Intelligence: An Epistemological Contribution to the Understanding of Intelligence", Intelligence and National Security, 28:5, pp. 694-716.

55. Warner, Michael, (2002), "Wanted: A definition of "intelligence"", Studies in Intelligence, 46, N.3..

56. Warner, Michael, (2009), "Intelligence as Risk Shifting", in Gill, Marrin, Phythian (Eds.) (2009), Intelligence Theory – Key Question and Debate, Routledge, London.

57. Warner, Michael, (2017), "Analysis as history, and history as analysis: a search for common goals and standards" *Intelligence and National Security*, 32(5), 613-624.

THE IMPACT OF LEISURE TIME POLICIES ON ECONOMIC SECURITY

Ileana-Cinziana SURDU*

Abstract

The economic security implies both the objective and the subjective perspectives, both the individual and state aspects, and it is dependent to the stability of the economy, as a result of adapting to the society's needs and evolutions in the context of labour market, opportunities, risks or competitiveness. The economic security represents an important aspect of the state's security status. As such, it becomes a field analysed in relation to social vulnerabilities and emergent changes at individual, the community and the society level.

The contemporary societies, and especially young people, manifest the need for individual leisure time, for free non-working time in order to do the activities they desire or plan, for spending time with the significant ones and so on. The new generation has replaced the past years' generations, for whom the working time represented the central aspect of their lives; the new generation values the leisure time, both the qualitative and the quantitative aspects. A paradox is met here: while trying to escape from the institutional limits of time schedule implied by a working program, the leisure time is managed by leisure industries.

In order to keep its functional aspect and to continue to follow a progressive process, the labour market has to adapt to the new generation's needs and desires in relation to the flexibility of their working schedule and to the stable character of the working place.

Economic security implies the protection from job and income instability, among other aspects like insurance etc. It is seen as "a public good". *The study considers the life standards perspective of the economic security concept, defined through individual and community dignity and fulfilment, in relation to the leisure time policies of the working place.*

The article analyses the degree in which the leisure time policies have an impact over the economic security of the individuals, defined through the subjective and objective perspectives.

*PhD student, University of Bucharest, The Faculty of Sociology and Social Work, Doctoral School of Sociology - ileana.cinziana.surdu@gmail.com; ileana.surdu@sas.unibuc.ro

The analysis reflects on leisure time policies and actions implemented by institutions and employers, in order to respond to the employees' demands regarding the working schedule, the flexibility of working time and also the stability of the job.

Keywords: *leisure time, leisure time policies, economic security, working time, individual economic security, state economic security.*

Argument: How do leisure time policies and economic security merge?

The contemporary societies, and especially the young generations, manifest the need to have a fulfilling career, a fulfilling personal life, a fulfilling family life, desires which come into contradiction to the available free time (Honoré, 2008).

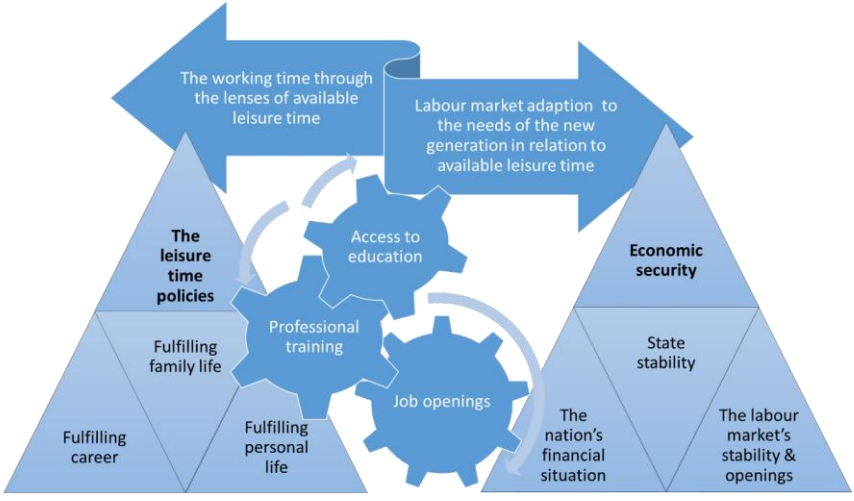
The economic security targets the stability of the state's situation, in relation to the nation's financial possibilities and through the stability character of the labour market and to its flow of openings. The most insecure social categories on the labour market are women, youngsters, rural residents and part-time employees. While the economic security status of rich nations is discussed through the financial possibilities, the developing countries are analysed through the high unemployment rate, and the economic dependency of people to the help of family members or other people who they can rely on from a financial point of view. (UNDP, 1994)

When facing economic insecurity, translated mainly as poverty, people turn to the national authorities for help. Economic security becomes more stable in the context of access to education, to professional training and to job openings (UNDP, 1994).

The new generation changed the perspective of old generations regarding the centrality of their working time into their lives and turned their interest to the amount of leisure time that the working schedule can allow them to have (Twenge et al., 2010). The youngsters find the stability of a job and the flexibility of their schedule more important than the salary (Florida, 2002).

In this new context, as sketched in the figure below, in order to continue to function properly, the labour market must adapt to the needs and expectations of the new generations, in relation to the amount of leisure time.

Figure 1. The flow between leisure market policies and economic security[1]



The article analyses the influence of the leisure time policies and values on the actions that provide the economic security of individuals, from a subjective and an objective point of view. To this manner, the discussion also reflects on the economic security of the state as complementary to the individual's economic security. The study discusses the policies and actions developed and implemented by institutions and employer entities in order to respond to the needs of the individuals in relation to the income necessities, reflected on the flexibility and stability of a job's characteristics and on the work-life balance. Consumption necessities are also analysed and discussed in relation to the developments of dedicated industries and services.

The article reflects on the leisure time policies as a component of the economic security of the individuals, in relation to the access to income opportunities and consumption alternatives.

What is economic security and how is it defined in relation to the state and the individual?

Helen Nesadurai (2004) proposes the analyses of economic security, not as a source or as a power instrument, but through the lenses of capitalist

[1] Source: Adaption after Honoré (2008), UNDP (1994), and Twenge et al. (2010).

production and equity. The author considers the globalization as context for addressing economic security, in relation to one's income level and stability, well-being and equal access to opportunities. Appropriate responsible institutions who can serve the interests of economic security are considered at national, regional and at global level (Nesadurai, 2004). But what effect has had the globalization on economic security, and how has it influenced the individuals, the societies and the states? And which type of institutions are appropriate for working in the interest of economic security? These are two main leading questions that Nesadurai (2004) considers in her analysis.

But first, what is "economic security"?

According to Kolodziej (1992), the realist approach relates the concept to military force aspects, like development or conflict. At the same time, the neorealist approach sustains the employment of national economic policies at international level (Moran, 1993). In order to highlight the importance of economic security, development studies have defined "economic insecurity" in relation to the vulnerable response of states and individuals to economic events, as for example economic crises, or losses (Scholte, 2000). The neoclassical approach considers that the economic flows, increases and decreases, are part of a natural course of economy. The globalization process has kept the economic security issues on the top of many states' agenda (Nesadurai, 2004).

The globalization process has brought both positive and negative implications on the economic security, making states' economy interdependent, and, as such, having implications on the design of economic policies (Nesadurai, 2004). Kolodziej (1992) underlines the fact that the status of economic security of a state, while being interconnected at international level, it is dependent of the state's history and strategic position and relations.

Baldwin (1997) concludes that after the end of the Cold War, security has started to be understood also in non-military terms, reaching to the population's realities and needs. The security studies have been divided into national security, human security, societal security and global security (Buzan, 1991). This non-military perspective includes areas like health, the environment protection, crime, or economic falls (Nesadurai, 2004).

After 1980, the analysis of security has started to include on a regular basis economic aspects also (Walt, 1991), including resources, development and risks. One of the main issues followed by states was the effect of trade (Harris and Mack, 1997), of economic dependency and of competition on the state of security of a nation (Zoellick, 1997/1998). Nesadurai (2004)

highlights the fact that the view on economic security has its roots in the traditional military approach, and that it may be relevant to current concerns of certain states or societies, as a result of the historical and social contexts.

Several definitions of economic security at the individual's level, including the human community, emphasizes on the stability of one's financial income resources, in order to maintain a quality life standard for the present and for the future period of time (Rupert, 2007).

From a subjective perspective, economic security implies the absence of fear in relation to the stability of known life standards, while from an objective point of view, it reflects the absence of fear that the known life values will be challenged or changed (Wolfers, 1952).

The economic security is dependent on the modernization of state economy and its characteristics in relation to ways of solving the modern challenges and threats, having as main purpose the insurance of the interests of the society (Grigoreva & Garifova, 2015). As one of the factors of the state economy, economic security is depend on the territorial resources, natural resources, development potential at social level, but also on the degree of development of new technologies (Grigoreva & Garifova, 2015).

The political perspective on economic security is in concordance to the realism approach, highlighting as sources of conflict the different interests of groups within a society. This is an important aspect when discussing economic security, in relation to the capitalist characteristic of the economy and to the way the market rules the economic security interests (Nesadurai, 2004).

The literature that analyses the state economic security identifies several defining components of the concept, as part of two categories: internal and external subsystems. The internal category relates to (Mkrtchyan, 2015):

- the technological aspect, which refers to the ability of the state to contribute to the technological progress and to be present on the international market with national technological products;
- the commercial perspective analyses the import and export capabilities of the state;
- the financial component describes the state's economic stability status and capabilities.

The external category includes:

- the technical component, which ensures the independency of the country in relation to the society's needs;
- the food and raw material perspective implies the provision of the necessary quantity of food and raw materials, at national level;
- the energetic security ensures the necessary provision of energy for use at national level;

- the ecological aspect refers to the ability to protect the environment;
- the informational security in all relevant areas, such as communication, politics, military, economy or social environment.

Mkrtchyan (2015) argues that the components of the state economic security are interconnected, and, moreover, are dependent to the changes that occur within a state at different levels: political, military, economic, social etc.

Liew (2000) identifies two main components of economic security: the micro one has as main subject the individual's access to means if income and consumption; the macro component reflects on the ability of the market to ensure the access to economic opportunities.

The current approaches on security studies emphasize on the domestic sources of conflict, like social differences, disparities, inequality. Economic security may be understood also in relation to the social contract between the society and the state, by approaching processes directed to decreasing the people's fears and to maintaining the already rooted values, like social stability and territorial integrity (Nesadurai, 2004). According to Buzan et al. (1998), protectionism is rejected in terms of ensuring economic security, because of the danger that can represent to market competition. This characteristic actually sets out the limit of economic security and the degree of allowed involvement of policy makers or of stakeholders in the field.

Economic development is understood as a main key in ensuring a state's security, but it cannot be automatically connected to the groups or individuals feeling of security, and in some cases it may also lead to conflict of interests, marginalization, and a rise of the degree of vulnerability (Nesadurai, 2004).

Globalization is often seen as a process with positive effects on the internal domestic economic security, by sustaining the international interaction between states. On the other hand, the negative effects of globalization are discussed in terms of illegal actions and trades (Nesadurai, 2004).

The national, regional and global institutions are considered a mix of entities that equally can contribute to ensuring the economic security within a state. These institutions can contribute to the economic security reported to the impact of globalization by: "(a) providing insurance, (b) aiding policy credibility and (c) encouraging policy adaption" (Nesadurai, 200, p. 18, acc. to Kahler), relying mainly on policies to this regard. Rodrik (1998) argues that the domestic institutions have an even greater role in case of conflict or economic disruptions; in order to be effective, they must present a democratic and non-corrupt character. In case of external disruptions, economic security can be reached and maintained only by an effective partnership and cooperation with other states (Nesadurai, 2004).

Economic security as a "public good"

Economic security is considered a "public good", when analysed through its role of ensuring stability to humans in relation to their job and monthly income, among other related aspects, such as life insurance. The Human Security Study Group (2007) emphasizes the principles of human security, identifying economic security as one of the component factors of human rights protection.

Barry Buzan (1983) finds no connection between individual and national security, as the state is the entity that ensures the individual security. Inevitably, the individual senses threats, either from the state itself, or born out of side-effects of the state's actions in order to create a secure environment. The author argues that for the individuals, the security gains meaning independent of the state, and it can also determine both problems and determining boosters for the actions taken by the state.

There are views which consider that economic security determines human security, and others that see the two concepts as being opposite. When discussing the security in relation to the individual and referring to the labour or the consumption markets, it can be related to the economic security of the whole community. Any type of interference I terms of attempt to install economic security for the community and for individuals could disrupt the course of the economic market. For instance, neoclassical views point out that economic insecurity can be motivational in terms of integrating on the labour market (Nesadurai, 2004).

Human security and economic security, are, thus, seen as being complementary: while economic security reports to the individual, the market is a referent of the macro-level security, allowing the individuals the access to a legal exploitation of the income and consumption possibilities offered by the market. On the other hand, applying the principle of equity within the rules of market is a must, in order to ensure the access of individuals and their progress in terms of income and consumption. (Nesadurai, 2004)

The human security studies consider the individual as the main beneficiary of the planned and implemented actions, realising him from two main concerns: fear and want (Nesadurai, 2004). The Human Development Report (UNDP, 1994) lists seven main categories of threats to human security: economic, food, health, environmental, personal, community and political. The economic security can be ensured mainly by a stable income. Because the labour market has become more and more instable, rich nations are characterised by the fear of not being able to find or to keep a job. The concept of job-sharing has installed itself as a fact in the industrialized societies. It is

not the case for developing societies, where unemployment rate is the measuring unit for economic insecurity.

A high unemployment rate can determine serious political and ethnic tensions. Also, the lack of social safety procedures, the poor individuals cannot manage to live without a regular income source. Family or community support often represent the safety net of this type of individuals, but only for a short period of time, so they find themselves in the situation of being forced to accept any type of job opening (UNDP, 1994). UNDP (1994) identifies as the most insecure categories, in relation to income stability, the farmers, the disabled, and the self-employed. Economic insecurity has negative effects over the population, out of which the most severe one is homelessness, especially in developing countries (UNDP, 1994). Human security protects the individuals "from sudden and hurtful disruptions in the patterns of daily life – whether in homes, jobs or in communities' and 'safety from chronic threats such as hunger, disease and repression" (UNDP, 1994, p. 23).

Leisure time policies and industries: the need for flexibility for an economic security

Nowadays, people aim to gain and maintain equilibrium between their time they allocate to their professional activity and to their personal and family life. Because leisure time does not represent any importance to the development process within a society, the modern capitalism show importance to the working time and activities. John Urry (1994) analyses the leisure time in relation to the working time, as it surely implies working activities for the industries that organize and offer alternatives of spending leisure time. Among this type of activities can be mentioned as organizing entities hotels, restaurants, parks, workout centres etc.

Traditional societies were characterized by the clear delimitation of the working time and leisure time, because of the stability of the working schedule. The non-working time has gained the characteristic of the time to spend money, which determined the development of the industries that offer different possibilities of leisure activities. Especially the private sector has focused on this type of activities, but, in a lower measure, so has the public sector. If the pre-industrial society used to organize them the working and the non-working time, the industrial society has become dependent to the formal economy for coordinating the two types of time. (Robertson, 1985)

Leisure time has become a valuable asset for the new generations, in contradiction to the traditional ones, for which the working time represented the central aspect of their lives. The contemporary society manifests a desire to have the necessary time to spend quality time with their significant ones, to

do individual activities that they wish and to be able to plan these activities in advance. The 19th century has launched the leisure time industries, especially in Great Britain, when people started to define leisure activities and to prioritize them in their lives (Whipp, 1987). From then, the economy has developed continuously, in order to offer alternatives for the new preoccupation of the individuals, which was their leisure time.

A study conducted by Twenge, Campbell, Hoffman and Lance (2010)[2] shows that for the new generation leisure time represents a life value, and the working time became no longer the main activity of their daily lives. The changes within the population's life values have brought changes within the values of employing industries and within the economic security field. Thus, some companies pay special attention to the balance between their employees' personal and professional life, and put at their disposal different services for relaxation or for solving household chores. For example, Google offers services for doing the laundry and for getting massages, eBay offers facilities for meditation and KPMG offers a longer vacation period during the first ear of employment.

Semco Corporation has understood the importance of a flexible working time and location in balance with the employers' motivation to work: the leader has offered the liberty of decision and action, the liberty of organizing the working schedule and to choose the working place, aspects that resulted with the efficiency of work and with financial gain. The same corporation has implemented internal leisure time policies in order to achieve a balance between the professional and the personal lives of its employees, by offering paternal leave long before it was implemented at public level, by offering a flexible working schedule and by strictly separating the communication channels used by the employees for work and for personal reasons. (Semler, 2003)

The industries have become more flexible in relation to offering possibilities of income and of consumption. By understanding the needs of the new generation of having time for family and individual activities and time, the labour market can determine the higher motivation for efficiency. According to Twenge et al. (2010), the employment entities are going through structural changes, in order to rely to the new social and life values in relation to the leisure time. These changes include the flexibility of working schedule and location, human resources internal policies, or motivational services.

[2] The study has been conducted on a representative sample at national level in the United States of America, in 1976, 1992 and 2006, with a total of 16507 of high school graduates, offering the possibility of comparing the results obtained within different generations of respondents with similar characteristics.

An interesting aspect when discussing economic security in relation to the income issues is represented by the level of integration of women on the labour market, in the context of the (still) traditional cultural expectations towards the gender roles in developing countries. To this respect, the factors that have led to the promotion of women on the labour market (such as the long life access to education, the flexibility of working schedule and policies regarding maternity leave and care) have also determined the need for a flexibility of the economic security in terms of consumption, and the development of dedicated policies and industries.

Leisure time policies can be currently related to the differences between women and men on the labour market, cultural gender differences within the household and work-life balance actions and policies.

Women tend to prioritize their family life to the detriment of their professional life. The tendency for women to dedicate their time to children and household chores to a higher degree than men, has been observed mainly in the case of low or medium income families, while families with higher income levels manifest the habit of relying on specialized services and industries to this manner. The social expectations and the gender stereotypes have a strong impact over the involvement of the women on the labour market (Bryson, 1999).

The European Commission targets the inclusion on the labour market of 75% of women and men until 2020, action which will contribute to the inclusion of women and to the work-life balance (European Commission, 2015). A series of actions implemented within the European Union and its Member States (MS) have targeted the obtaining of a work-life balance and the assurance of equal access of women on the labour market and to leader positions. From 2011 the European Commission has implemented the Mutual Learning Programme in Gender Equality, presenting and discussing opportunities and barriers connected to subjects such as the access of women in the political field, the labour situation of single parents, the gender segregation on the labour market, a flexible working schedule, the role of men in obtaining gender equality, or the work-life balance (The European Commission, a).

Work-life balance policies and actions that the European Union promotes can be divided in three main categories: the flexibility of the working schedule, support for raising the children and caring services. In 2015, the European Commission has launched the campaign "New start to address the challenges of work-life balance faced by working families". The initiative targets the development of European policies which could (a) offer the frame for a work-life balance for parents with young children, (b) promote

equal dedication of men and women within the household, and (c) promote equity on the labour market. (European Commission, b)

Also in 2015, The European Commission has launched "Strategic Engagement for Gender Equality 2016-2019". The strategy discusses five aspects of gender equality: economic independency, equal pay for equal labour, involvement in decisions, integrity and dignity, promoting gender equality outside the European Union. (European Commission, c)

This type of policies may have a positive impact on economic security of individuals, registering results at the level of involvement of women on the labour market, at the level of access of men and women to positions in concordance to their level of education and professional training, at the level of independency of working individuals, and it may have as main result the reduction of risk of poverty. At the same time, the policies may have a positive influence at the level of employment entities also, by having access to more qualified and motivated labour force, by registering more efficient results and a higher productivity level. (European Commission, 2015)

Conclusions

The article has addressed the impact of leisure time policies and actions over the status of economic security of individuals, in terms of access to income opportunities and consumption alternatives. Both the subjective and the objective perspectives of the economic security have been analysed to this regards.

The analysis reflected on aspects of human development through the perspective of human security, which opens new opportunities of understanding certain aspects of life in an informative way, as Oscar and des Gasper (s. a.) argues in their paper. The progressive process of the labour market has proved to be dependent on the ability to adapt to the new generations' needs in relation to the work-life balance and the stability of the job. This can be translated (among other aspects) into the flexibility of the working schedule and place, into the implementation of gender equality policies on the labour market and within the household, into the access to services for supplementing the household chores and the care of children, and also into access to industries dedicated to spending the leisure time.

Being considered "the time for spending money", the leisure time determined the development of dedicated industries and structural changes within employing industries, offering possibilities and alternatives for both income and consumption, according to the needs, life values and standards of the new generations, trying to eliminate the feeling of "fear and want", thus ensuring the economic security of individuals and of the state.

References:

1. Baldwin, D. A. (1997). The concept of security. *Review of International Studies*, *23*, 5-26.

2. Bryson, V. (1999). *Feminist Debates. Issues of Theory and Political Practice*. London: Macmillan Pres Ltd.

3. Buzan, B. (1983). *People, States and Fear. The National Security Problem in International Relations* (2nd ed). London: Wheatsheaf Books LTD. 2nd Edition.

4. Buzan, B. (1991). *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*. Boulder, CO: Lynne Rienner.

5. Buzan, B., Waever, O., de Wilde, J. (1998). *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner.

6. European Commission (a). *Mutual Learning Programme in Gender Equality*. Retrieved from: http://ec.europa.eu/justice/gender-equality/other-institutions/ good-practices/index_en.htm

7. European Commission (b). *Professional, private and family life*. Retrieved from http://ec.europa.eu/justice/gender-equality/rights/work-life-balance/index_en.htm

8. European Commission (c). *Gender equality*. Retrieved from: http://ec.europa.eu/justice/gender-equality/index_en.htm

9. European Commission. (2015). R*oadmap. New start to address the challenges of work-life balance faced by working families*. Retrieved from: http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_just_012_new_initiative_ replacing_maternity_leave_directive_en

10. Florida, R. (2002). *The Rise of the Creative Class. And How it's Transforming Work, Leisure, Community and Everyday Life*. New York: Basic Books.

11. Grigoreva, E., Garifova, L. (2015). The economic security of the state: the institutional aspect. *Procedia Economics and Finance*, *24*, 266-273. Retrieved from www.sciencedirect.com

12. Harris, S., Mack, A. (1997). *Security and economics in East Asia*. In Stuart, H., Mack, A. (eds). (1997). *Asia-Pacific Security: The Economics–Politics Nexus*. St Leonards, NSW: Allen & Unwin, 1-29.

13. Honoré, C. (2008). *Elogiu lentorii: o provocare adresată cultului vitezei*. Bucharest: Publica.

14. Kolodziej, E. A. (1992). Renaissance in security studies? Caveat lector! *International Studies Quarterly*. *36*(4), 421-38.

15. Liew, L. (2000). Human and economic security: is there a nexus? In William T. T., Thakur, R., Hyun, I. (eds). *Asia's Emerging Regional Order: Reconciling Traditional and Human Security*. New York: United Nations University Press, 192-208.

16. Mkrtchyan, T. M. (2015). *State Economic Security System and Its Components*. 4th Int'l Conference on Research in Humanities, Sociology & Corporate Social Responsibility (RHSCSR'15) Sept., 2015 Penang (Malaysia), 25-26. Retrieved from http://dx.doi.org/10.15242/ICEHMED915013

17. Moran, Th. (1993). An economics agenda for neo-realists. *International Security*, *18*(2), 211-15.

18. Nesadurai, H. (January, 2004). Introduction: Economic security, globalization and governance. *The Pacific Review*. *17*(4), 459-484. doi: 10.1080/0951274042000326023

19. Oscar, A. G., Des Gasper. (s. a.). *Human Security. A Thematic Guidance Note for Regional and National Human Development Report Teams.* United Nations Development Programme Human Development Report Office.

20. Robertson, J. (1985). *Future Work: Jobs, self-employment and leisure after the industrial age.* Aldershot: Gower Publishing Company Limited.

21. Rodrik, D. (1998). *Where did all the growth go? External shocks, social conflict and growth collapses*. Working Paper 6350. Cambridge: National Bureau of Economic Research. Retrieved from https://www.nber.org/papers/w6350

22. Rupert, M. (2007). *International Relations Theory*. Oxford: Oxford University Press.

23. Scholte, J. A. (2000). *Globalization: A Critical Introduction*. New York: St Martin's Press.

24. Semler, R. (2003). *The Seven-Day Weekend. Finding the Work-Life Balance*. London: Century.

25. The Human Security Study Group. (2007, November 8). *A European Way of Security. The Madrid Report of Human Security Study Group comprising a Proposal and Background Report*. Retrieved from http://fdm.rio20.net/sites/default/files/IMG/pdf_0078_A_European_Way_of_Security.pdf.

26. Twenge, J. M., Campbell, S. T., Hoffman, B. J., Lance, Ch. E. (September, 2010). Generational Differences in Work Values: Leisure and Extrinsic Values Increasing, Social and Intrinsic Values Decreasing. *Journal of Management*, *36* (5), 1117-1142. Retrieved from http://www.sagepub.com/journalsPermissions.nav

27. United Nations Development Programme (UNDP). (1994). *Human Development Report 1994*. New York: Oxford University Press. Retrieved from http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf.

28. Urry, J. (June, 1994). Time, Leisure and Social Identity. *Time & Society*. 3(2). Retrieved from http://tas.sagepub.com/content/3/2/131

29. Walt, S. M. (1991). The renaissance of security studies. *International Studies Quarterly*. *35*(2), 211-39.

30. Whipp, R. (1987). A Time to Every Purpose: An Essay on Time and Work. In Joyce, P. (ed.). *The Historical Meanings of Work*. Cambridge: Cambridge University Press, 210-36.

31. Wolfers, A., (1952) "National security" as an ambiguous symbol. *Political Science Quarterly*, *67*(4), 481–502.

32. Zoellick, R. C. (1997/1998). Economics and security in the changing Asia-Pacific. *Survival*, *39*(4), 29-51

THE COLLISION BETWEEN PUBLIC POLICY AND TECHNOLOGY RAISES THE STAKES FOR USERS

Claudia GOGOAŞA LASCATEU*

Motto: *"Salus populi suprema lex esto"* [1]
(Iustinian I, 482 –565 a.D.)

Abstract

Strategy, public policy and threat management have risen and flourished despite the constant conundrum of protecting infrastructure and top technology. To have both the big picture and successfully prevent or interrupt malicious behaviour it is necessary to comprehend what the threat is and what it means to us, and to achieve that, we must be able to position ourselves between grasping what public policy has to offer and what technology brings to the table.

This is intended to be an interdisciplinary approach on law and policy that will show what are the limits and guarantees of user experience nowadays in the European Union and, secondly, will argue the advantages and disadvantages to what are users experiencing in non-member states.

The paper will analyse what part data and confidentiality for security plays and how a continuous development of policy and strategy can answer the questions raised by technology and hybrid threats to national security. It will follow the lines European policy draws given the latest threat development and will revolve around what changes form the user's perspective.

Therefore, from necessity to strategy, to enforcement, the first step is identifying and addressing one issue in a common manner. Furthermore, it means we can achieve common grounds and have a correct and adequate solution. In order to find out how public policy works better for individuals, we scrutinise whether the European General Data Protection Regulation (GDPR) is an answer to all our questions, or just a complex insurance designed to safeguard user online experience. Moreover, we study how enforcing an internet law like China or Russia is in comparison to having a set of rules and guarantees such as the European GDPR, and the effect on user digital behaviour.

* PhD candidate, "Mihai Viteazul" National Intelligence Academy.

[1] "Let the safety of the people be the highest law", Cicero, De Legibus, Loeb Classics, p. 467.

The basis of this study will approach European case law on the matter of guaranteeing user fundamental rights concerning confidentiality, showing how European strategy is being enforced by regulations and put into force by law. It also finds that member states have the inherent responsibility to guarantee both user rights and transparency.

To have a better understanding on how people perceive the rules and regulations we use polls to measure how the public policy framework is comprehended by the people it intends to protect, and if the state policy toolset guarantees users digital literacy.

Keywords: *user, privacy, personal data, law.*

Introduction

The right to have a protected intimate, family and private existence is complex and is guaranteed by the Romanian Constitution from the outset as a supreme value (Article 1 of *Romanian Constitution*, 2003), further enhanced by the complementary obligation of state authorities to respect and guard individuals and their privacy (Article 26 of Romanian Constitution, 2003). The state, through public authorities must employ whatever means necessary within reason to guarantee privacy of individuals as fundamental human right. These have roots in the International Covenant on Civil and Political Rights (ICCPR)[2] Article 17 which states that nobody can be subject to arbitrary or illegal pries in his private life, family or home, neither can be unlawfully offended in his honour or reputation. Every person has the right to be protected by the law against such transgressions.

Furthermore, the Romanian New Civil Code states that anybody has the right to live, to be healthy, to have mental and physical integrity, to have dignity, to have self-image, to have his private life respected, and these rights cannot be transmitted (Article 58 of the *New Romanian Civil Code*). These are fundamental human rights, guaranteed by the Romanian Constitution sprung from the International Bill of Human Rights. The Romanian law states that anybody is entitled to have a name and a place of residence legally obtained. So, these attributes are not guaranteed, as they are conditioned by the pursuit of legal procedure, but are qualities that are constituent of the fundamental right to live and have a private life.

[2] It is a multilateral treaty adopted by the United Nations General Assembly through GA. Resolution 2200A (XXI) on 16 December 1966, part of the International Bill of Human Rights, ratified by Romania in 1974 by Decree no. 212.

The limits and guarantees of user experience nowadays in the European Union

The protection of user privacy as a guarantee stated in Article 8 of the Human Rights Convention and Article 16 of the European Union Treaty is now better outlined and linked to responsibility and the requirement to implement a system of protective measures that cover both data bases with personal data and the limits and conditions of third-party exchanges.

For instance, the Romanian law has included a general interdiction (Article 65 paragraph 2 of the *New Romanian Civil Code*) for identification of a person based on his genetic fingerprint outside of a civil or penal suit or in a medical or research matter. It is concordant with the European Human Rights Courts` jurisprudence that basically outlines in the 2006 *Van der Velden v. the Netherlands decision* that Article 8 in the Human Rights Convention the right to respect one`s privacy covers the issue of retention of data related to biological features of an individual, beyond the scope of its submission in the first place, because it is protected under the 1981 *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*.

Restrictions come with sanctions directly linked to the way technology has developed and how online user interactions have proven to function nowadays. The former Directive 95/46/CE has fallen behind to being in accordance with the pace of digital environment and the way society has blended in the cyber world.

The legitimate purposes of harnessing private user data must respect the GDPR (The General Data Protection Regulation (EU) 2016/679) indifferent of the area of expertise it addresses. Commercial, political or administrative purposes are bound to address each user in a transparent manner stating the extent of processing the data provided by every person. Denial of data processing should not restrict or affect user`s access to public domains or reduce the amount of content is accessed on the account of whether permission to harness personal data is granted.

An infringement of privacy is considered necessary in a democratic society to reach a legitimate goal if it answers an essential social request, and especially if it is proportionate to the legitimate scope envisioned by the authorities to justify the limitation of privacy rights is pertinent and adequate as the European Court for Human Rights has concluded in *Coster v. United Kingdom* in 2001.

The Romanian law states that anybody has the right to have his private life respected (Article 71 the *New Romanian Civil Code*), and that nobody can be exposed to any kind of indiscretion to his intimate, personal or family life, in his

home or correspondence, without his consent or with disregard to the restrictions and limits imposed by national law or the treaties Romania has assumed. (Article 75 the *New Romanian Civil Code*). It`s also forbidden to use in any means the correspondence, manuscripts or any other personal documents, private information regarding someone without his consent or with disregard to regulations (Article 71 the *New Romanian Civil Code*).

Private life, as it is perceived by the European Human Rights Court in the 2004 *Von Hannover v. Germany* decision, is formed of elements that are directly linked to a person`s identity such as name, picture or image, physical and moral integrity. The guarantee stated by Article 8 of the Convention is mainly aimed at ensuring the development, without outside input, of each individual`s personality in relation to his keen.

Private data should not be used as currency, it is part of each person`s individuality. Like copyright, personal data can be leased but not transferred, the owner/user has the fundamental right to choose how it should be used, as this type of data persists as long as the person is alive and cannot be worn out. Despite that it has proven to be valuable merchandise for illegitimate harnessing and trade intended for generating patterns of predictive behaviour in order to micro target narratives to influence voters in political campaigns in EU states and USA the last elections.

Anybody has the right to have his dignity respected, any affliction of one`s honour or reputation is forbidden apart from given consent or outside the limits set by the Romanian law (Article 72 the *New Romanian Civil Code*). The right to have a reputation is part of private life as European Human Rights Court has settled in the 2007 *Pfeifer v. Austria* decision. One`s reputation is part if his personal and psychological identity and are the subject of one`s private life.

Personal data cannot be relinquished, but users have the right to be forgotten by the cyberspace. It doesn't mean their data disappears, it only means search engines and data base administrators will delete and not show the results related to any of the private data linked to that user.

What is interesting is that the GDPR applies also to non-members of the EU that are processing data of European residents, meaning it also changes third-party policy that is interlinked to goods and services on European market. It not only applies to policy, but it forces third-party operators to comply, due to harsh international reach of penalties imposed by the GDPR. (Rödl & Partner, 2018)

What are users experiencing in non-EU-States

India has not defined the principle of privacy in its Constitution, but has set the legal framework for Information Technology since 2000 and improved security practices and procedures by 2011 at which point sensitive personal data and information have taken an important role in this country`s revenue. So, the 2011 Rules are basically implementing the principle of responsibility for data collectors, the principle of transparency regarding the type and purpose of sensitive data collected and stored the principle of users` consent and the guarantee of data security. What Indian authorities consider sensitive information are biometric data, medical records, sexual orientation, banking history and any other piece of information that is not publicly accessible. These Rules have in fact a similar effect to what the outline of the GDPR is intended to have; only that it addresses Indian residents (Rödl & Partner, 2018).

In august 2018, the Indian authorities have drafted the framework of personal data privacy in a bill that should align to the standards of safeguarding users and support its ever-growing digital economy, by forming an independent regulatory body that should enforce data protection law and apply penalties, both to private and public sector, bearing in mind that India`s online market is only second to China`s (Balaji, 2018).

India is taking effective steps to align to European privacy policy in order to maintain trade and economic growth, proving once again that public policy is aligned to national strategy, despite other national issues and policies regarding the protection of human rights that are still a few steps back.

For comparison, the **Chinese** users have the full up-to-date legal framework to safeguard their private date hence numerous corporate and governmental data experience, but, in fact, their legal guarantees are only a part of making efficient steps toward data privacy, since Chinese illegal data transactions increase. To manifest, in April 2018 an artist called Deng Yufeng bought and included in his exhibit private data of 346,000 Chinese people (Hersey, 2018), authorities closed his art exhibition in 2 days and pursued charges.

Research on personal privacy protection in China shows that privacy content changes accordingly to background and culture, and nowadays Chinese consider that the most important personal data is the ID number, and the second is the personal phone number (See more on Zhao and Dong, 2017).

Similar to the European point of view regarding personal data, Chinese consider real names, home address and IP address an important constituent of personal data that needs to be protected by those who receive and store such

information, meaning in fact, private operators. In 2017, the Chinese Network Security Law enunciates the principles that govern data collection and the standards that should be met by any entity that collects private data. What is interesting is that the government outlined that data collection should firstly be legal, justified and necessary, then collection should be minimal, retention should be short, and usage should be within minimum scope (Udemans, 2018) the same way the European Parliament states in the GDPR.

China takes a step forward to assessing it`s citizens` private data by piloting a Social Credit System which is intended to come into force by 2020 that should be based on big data analysis technology and is intended to raise social awareness to achieve integrity as it is viewed by authorities (Botsman, 2017). The endeavour is heavily disputed, and it remains unclear how authorities will guarantee a useful toolkit to serve its citizens benefit given that it remains to be clarified in what respect the users can dispute their social score. This metadata governmental collection has taken user privacy beyond what other states are achieving through effective public policies and democratic process.

The **United States of America** data protection framework is not governed by a single principal data protection law; the protection is granted by enforcing both national and state level regulation and is achieved in different sectors by specific measures. Other states have enforced specific procedures to generally safeguard personally identifiable information of their residents. (*Data Protection 2018*) Most interestingly is that American privacy regulations are emergent from consumer protection law intended to discourage prejudicial practices, while other countries only apply policies like GDPR in order to maintain compliance and keep commercial trade on its rising course, user privacy as principle being barely emergent in national law.

A cornerstone in user privacy protection in USA was reached in 2013 when after numerous governmental surveillance disclosures, authorities have drawn a line (*Accountability and Privacy Act of 2013*) in limiting the extent of state monitoring but also harshening procedure that must be abided. The Act has been criticised as a limitation of state powers but seen by public as a guarantee of human rights in the process of preventing terrorist attacks and foreign powers` unlawful intelligence operations.

Mexico for instance has privacy as a fundamental guarantee in Constitution, powered by national personal data law governed by the same principles as those outlined by the GDPR, since Mexico has been a signatory of the United Nations Universal Declaration of Human Rights 1948, and later treaties (*International Covenant on Civil and Political Rights*, 1966 and OAS

Inter-American Convention on Human Rights, 1965) to enforce and ensure the protection of human rights.

Regarding personal privacy from a European viewpoint, in 1997 Mexico adopted Directive 95/46/EC (1995) on data protection, as part of the Economic Partnership, Political Coordination and Cooperation Agreement with the EU, and later, in 2018 adopted the Strasbourg Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981 and its Additional Protocol regarding supervisory authorities and transborder data flows (*Privacy in Mexico*, 2018).

Despite the legal framework that Mexico has accessed, authorities are criticised for not being successful in implementing effective measures to guarantee privacy as a human right, lacking a successful toolset to have public scrutiny over government surveillance. (*Privacy in Mexico*, 2018; Ahmed and Perlroth, 2017)

How users comprehend the new standard

Even though the means of communication guaranteed by internet nowadays has its benefits, users of the network cannot be effectively protected, their private life being constantly subject of unsolicited messages, images or information. The inconvenience can be reduced but not thoroughly deterred by proving the minimum digital literacy and the installation of filters. It`s not enough to identify the breach of privacy rights for an effective outcome, pre-emptive measures must be established.

Receiving unsolicited e-mails with unsolicited content is not yet a matter that can be the subject of the state`s intervention and protection if the sender cannot be identified and made responsible. For instance, the 2007 *Muscio v. Italy* decision of the European Human Rights Court has established that if the author of the breech of privacy cannot be identified, there cannot be a punishment, and art. 8 of the Convention are not violated.

How are users supposed to be prepared to interact and communicate using these new mechanisms but also keep their individuality private has come to be a balance of digital competence gained throughout work related communication and self-taught digital abilities assisted by user friendly technology.

To have a better understanding on how people perceive the rules and regulations a poll was used to measure how the public policy framework is comprehended by the people it intends to protect, and if the state policy toolset guarantees users digital literacy.

In order to appreciate the way people grasp the rules that govern the on-line sphere and to accurately measure how the public policy outline is accepted by the public they are meant to protect, we have designed the basic profile of a user that has to deal with an afflux of data and ominous threats of the digital space.

Demographics, gender or age are not criteria that should have a saying in how the user interacts on-line, since public policy has no such exceptions, the criteria we have used in studying the level of knowledge of digital space one needs in connection to the abilities one requires to successfully operate the digital space has been whether it is work related or not.

In this hypothesis it is important for our society to differentiate between the requirements of keeping up with new technology and the new facts that change the way we work and inherently influences productivity.

What we find mainly in any user is the ability to communicate and interact. That is what defines the digital space, the way people communicate. It is important to observe how this takes an important part of any person's daily on-line activity. So, our study must start from measuring the level of development of ability to successfully communicate digitally.

63% of those who answered said that at work they use frequently the on-line communication platforms, saying that it turns the work dynamics in an easier and more efficient manner.

70,4% of the respondents said that their computer skills are concurrent with what the job description usually needs for their kind of job.

64,8% of those who answered use a proprietary platform in the organisation they work.

While only 61,1% of the respondents use sometimes only digital means to interact at workplace.

From the study's perspective, the user is a person who uses a computer or a service in a network. Typically, the people who use systems and software products are not technically skilled to fully grasp how these actually function, that is why communication abilities are transferred in the digital realm as far as the user comprehends the benefits the technology he accesses has to offer, and the limits it withholds. The level of digital literacy and the efficiency of time spent doing the same operation towards the same result are directly linked.

57,4% of the respondents say that their trainings are always directly linked to their jobs specificities, while 40,7% say that only sometimes the in-house training is directed to the job description.

43,3% of those who answered the poll only sometimes take part to varied training forms, while only 7,5% always have different learning experiences.

The level of comprehension and the possibility to harness all that technology has to offer differs in direct relation to the domain the user works, indifferent of the virtual regulations imposed. Having that in mind, an important factor in this study are the means of information and self-study one uses to adapt to new technology, and whether the individual drive to study or the workplace learning tools affect the level of knowledge and skill required by today`s digitalisation. As basic reference text processing, charts and multimedia presentations were selected.

40% of those questioned answered that they seldom study the latest news regarding technology through accessing demonstrative clips, forums, professional sites or publications.

Only 46,3% sometimes work with spreadsheets, and 35,2% occasionally use multimedia presentation apps.

To clarify whether there is a link between digital skills and the career orientated trainings we must further the analysis of the source of the user`s basic digital operating knowledge and the specific capabilities required by the present in the virtual space to correctly and efficiently identify the risks of the web.

The proof of having the ability to use nowadays a network system is that the user proves to know what data security represents. One of the most outspoken ability is to avoid spam, one of the most frequent risks that can affect not only personal data integrity, but also network functions of the organisation.

Thus, the study shows that only 40,7% of those interviewed always correctly identify unsolicited electronic commercial messages for shady products or services, marking them as spam, unsubscribing, blocking, ignoring or deleting without reading.

Also, 55,6% check all the time the data asked via e-mail by checking official information or other sources of information, while 18,5% pay attention to alarming messages aimed to get one's attention towards a plausible fact, asking further dissemination.

Moreover, a valued ability to accomplish digital literacy for a user is to follow up-to-date **confidentiality** standards.

9,3% always answer to personal data requests received on e-mail from acquaintances, while 55,6% never answer.

50% always study thoroughly digital messages received from appearance to content.

After studying the legal terms 14% always consent to granting access to their personal data to the operator, 55,6% only sometimes agree to granting access, while 24,1% rarely agree, and 5,6% never consent to sharing their private data.

What changes form the user's perspective?

An increase in *digital bureaucracy*, less spamming, the same amount micro targeting for commercial purposes using more sophisticated technology, fake news persists, greater transparency of social media regarding third-party access to user private data, better liability management, compulsory independent regulator of private data management.

Conclusion

The legal framework guarantees privacy, but to put into force what the principles state, technology must answer to the standards imposed and awareness should become a strategic outline. Knowledge is gained, not a given fact.

What policy should bring to the table is attracting structural investment in digital literacy, youth educational programmes in schools and adult focused trainings, to achieve effective means of safeguarding digital privacy.

References:

1. Azam, Ahmed, Perlroth, Nicole, (2017), *Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families*, The New York Times, June 19.

2. Balaji, Sindhuja, (2018), *India Finally Has A Data Privacy Framework – What Does It Mean For Its Billion-Dollar Tech Industry?*, Forbes, August 3.

3. Botsman, Rachel, (2017), *Big data meets Big Brother as China moves to rate its citizens*, Wired UK, Retrieved 26 October.

4. Cancino, Begoña, Creel, García-Cuéllar, Aiza y Enríquez, (2018), *Privacy in Mexico: overview*, Thomson Reuters Practical Law, July 1st.

5. *Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* (October 24, 1995).

6. *Data Protection 2018*, International Comparative Legal Guides, June 6.

7. European Court of Human Rights, *Van der Velden v. the Netherlands*, (2006), retrieved from http://echr.ketse.com/doc/29514.05-en-20061207/view.

8. European Court of Human Rights, *Coster v. United Kingdom*, (2001) retrieved from https://swarb.co.uk/coster-v-the-united-kingdom-echr-18-jan-2001.

9. European Court of Human Rights, *Von Hannover v. Germany*, 2004, retrieved from https://www.juridice.ro/wp-content/uploads/2016/07/von-Hannover-v-Germany-ECHR-24-June-2004.pdf.

10. European Court of Human Rights, *Pfeifer v. Austria*, (2007), retrieved from https://swarb.co.uk/pfeifer-v-austria-echr-15-nov-2007.

11. European Court of Human Rights, *Muscio v. Italy*, (2007), retrieved from https://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf.

12. *Foreign Intelligence Surveillance Act* (FISA), Accountability and Privacy Act of 2013.

13. Hersey, Frank, (2018), *Artist buys and exhibits black market data of 346,000 people, invites them to visit*, Tehnode, April 10.

14. *New Romanian Civil Code*, (2014).

15. Rivas, Diego, Mantovani, Chiara, (2017), *Lawful and unlawful surveillance in Mexican democracy*, Revista Internacional de Comunicación y Desarrollo, ENSAYO, 7, 111-129, ISSN e2386-3730.

16. Rödl & Partner, *Indian Data Privacy laws and EU GDPR*, (May 24, 2018).

17. *Romanian Constitution* (1991 and 2003).

18. *Romanian Decree 212*, (1974).

19. *The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, (1981).

20. *The General Data Protection Regulation (EU)*, 2016/679.

21. *The Universal Declaration of Human Rights*, (1948).

22. *The International Covenant on Civil and Political Rights*, (1966).

23. Udemans, Cristopher, (2018), *Chinese care more about data privacy than you think, but they still need better protection,* Technode, May 15.

24. Zhao, Hui, Dong, Haoxin, (2017), *Personal Privacy Protection of China in the Era of Big Data*, Open Journal of Social Sciences, ISSN Online: 2327-5960.

REVIEWS AND NOTES

Alina Bârgăoanu, #FakeNews. Noua cursă a înarmării, Editura Evrika, 2018, 252p (Recenzie de Mihaela Teodor)



Sursa foto: http://snspa.ro

În 2018, Alina Bârgăoanu, Decan al Facultății de Comunicare și Relații Publice din cadrul SNSPA, a făcut parte din grupul celor 39 de experți aleși de Comisia Europeană pentru a oferi consultanță Comisiei Europene cu privire la fenomenul răspândirii conținutului fals, definind rolurile și responsabilitățile părților relevante, evaluând dimensiunea internațională și riscurile și formulând recomandări în vederea extinderii sau introducerii de noi acțiuni. (Sursa: http://snspa.ro)

Profesorul Alina Bârgăoanu ne propune o carte introductivă în problematica reală a dezinformării și „știrilor false" (termen care nu acoperă, în opinia autoarei, traducerea *fake news*) din noua epocă digitală, scrisă într-un stil jurnalistic, cu formulări de stil iscusite care suscită atenția cititorului.

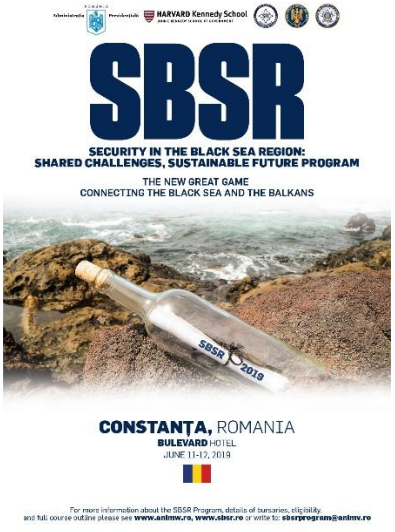
Lucrarea *Fake news – noua cursă a înarmării* este structurată astfel: o introducere (La răscruce de vremuri), șase capitole (Tehnologia este destin; Noi vs. Ei. Metropole digitale și periferii analogice; Noii despoți globali; Dezinformarea 2.0. Dezinformarea de nouă generație; Oamenii nu mai sunt puși în mișcare de alți oameni; Sufrageria digitală) și un capitol de concluzii (Leadership-ul intelectual configurează viitorul).

Primul capitol al cărții reprezintă o mărturisire personală cu privire la modul în care, tehnologiile au evoluat odată cu evoluția ordinii mondiale. În capitolul al doilea, autoarea propune o analiză pertinentă și lucidă a unor concepte, precum post-adevăr, dar și a unor fenomene precum recesiunea economică și criza financiară, care au dat naștere unei „recesiuni umane"

însoțită de populism. Acest fenomen este definit ca „un loc geometric pentru o serie de reacții emoționale dintre cele mai diverse – frustrare, mânie, nemulțumire – a cel puțin trei fenomene care se întrepătrund: globalizarea, integrarea europeană și tranziția de la comunism la economia de piață, dirijată de fantomaticul „"Consens de la Washington", de o rețetă neoliberală brutală" (p. 71). Citând o investigație a celor de la New York Times privind concentrarea capitalului în democrațiile liberale, Alina Bârgăoanu propune în capitolul al treilea tema „noilor despoți globali". Capitolul al patrulea, Dezinformarea 2.0, propune clarificări importante ale conceptului de "fake news", autoarea folosind un limbaj jurnalistic pentru traducerea termenului: „făcături" și „fonfleuri". Capitolul al cincilea analizează probleme ale epocii social-media, precum: comercializarea atenției noastre de către platformele sociale, a datelor personale și a profilelor noastre psihologice. Capitolul final abordează problema propagandei de stat cu trimitere directă la propaganda rusă și la fabrica de troli de la Sankt Petersburg, care au reușit să utilizeze platformele sociale într-un mod foarte inteligent în timpul dezbaterii electorale americane.

Cartea oferă o perspectivă nuanțată și complexă a fenomenului *fake news*. Fake news-ul este un fenomen care a dat naștere la un val de interes cu adevărat specataculos și la o modă, în lumea cercetării științifice din domeniul științelor sociale și nu numai. Totuși, volumul *#FakeNews. Noua cursă a înarmării* este unul scris cu rigoare academică, pe o bază documentară reală și cu caracter interdisciplinar, care dovedesc o lectură serioasă a fenomenelor politice, economice și sociale actuale.

ACADEMIC FOCUS



SECURITY IN THE BLAK SEA REGION: SHARED CHALLENGES, SUSTAINABLE FUTURE PROGRAM
Constanța – June 11-12, 2019

THE NEW GREAT GAME – CONNECTING THE BLACK SEA AND THE BALKANS

Over the past few years, the Black Sea Region and the Balkans have increasingly emerged as potential game changers in regional security. It has therefore become an undisputed fact that both the Black Sea Region and the Balkans are involved in a significant dynamic not only for European security, but also for the main actors of the international scene. These regions are major crossroads and critical intersections of the East-West and South-North corridors. Moreover, looking back in history, we can also state that the wider region including the Black Sea shore and the Balkans has always been considered an interconnector for Europe, Asia and Africa and a pivotal region for trade and geopolitical affairs. Time and again, experts stated that the one who dominates this region can easily project power both to the European continent, as well as in the Eastern Mediterranean, South Caucasus and the northern Middle East.

The 2019 edition of the international program – The New Great Game - Connecting Black Sea and the Balkans– will aim to evaluate the current situation in the Black Sea Region and the Balkans to identify the main challenges faced by the countries in these two regions in terms of security, stability and sustainable partnerships. The program will focus, therefore, on setting the scene to better understand current security, social and economic evolutions in the two regions and on collectively analysing and generating options for policy recommendations. The main goal of the SBSR Program is to

facilitate in the participants a transformative vision, turning challenges into opportunities for shared growth. The social, economic, political, and cultural and security issues at stake for resilient sustainable partnerships in the region are also brought into focus. The program is aimed to bring together, in an interactive and collaborative format, policy makers, security experts and foreign affairs officials from the Black Sea Region, the Balkans and their strategic partners. The Program will include lectures, debates, problem solving exercises and a policy analysis exercise (PAE).

The SBSR program is organized under the high patronage of the Romanian Presidential Administration, by the Romanian Intelligence Service's "Mihai Viteazul" National Intelligence Academy, in partnership with Harvard University and the National Intelligence University (NIU), US. To maximize output and valuable interactions between participants and experts in the field, this year's edition will be organized as a back to back event with the Black Sea and Balkans Forum to be held in Constanta, Romania, during June 13-14, 2019.

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, 2020)

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.

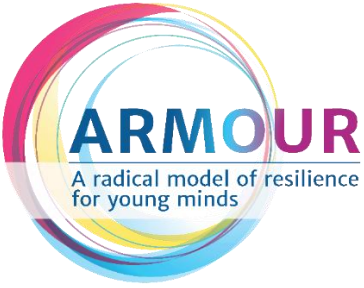
CRESCEnt project creates a training platform and a set of communication and cross-sectorial strategic communication instruments, which aim to capacitate institutional spokespersons and journalists from security and LEA fields, in order to use media reporting to the public in a conscious and ethical manner. 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, 2020)

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.

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. 21 and 22 and which is scheduled to be published on June and December, 2019.

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.**

Invited reviewers:

Sorin APARASCHIVEI
- Researcher, National Institute for Intelligence Studies, MVNIA Romania

Irena CHIRU
- Professor, "Mihai Viteazul" National Intelligence Academy, Romania

Cristina IVAN
- Researcher, National Institute for Intelligence Studies, MVNIA Romania

Ioan Codruț LUCINESCU
- Researcher, National Institute for Intelligence Studies, MVNIA Romania

Veronica MIHALACHE
- Associate Professor, "Mihai Viteazul" National Intelligence Academy, Romania

Cristian NIȚĂ
- Associate Professor, "Mihai Viteazul" National Intelligence Academy, Romania

Ileana SURDU
- Researcher, National Institute for Intelligence Studies, MVNIA Romania

Valentin STOIAN
- Researcher, National Institute for Intelligence Studies, MVNIA Romania

Bogdan Alexandru TEODOR
- Lecturer, "Mihai Viteazul" National Intelligence Academy, Romania

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