RISR No. 1 (29)/2023

ROMANIAN INTELLIGENCE STUDIES REVIEW

EDITURA ANIMV

"MIHAI VITEAZUL"
NATIONAL INTELLIGENCE ACADEMY

ROMANIAN INTELLIGENCE STUDIES REVIEW

No. 1 (29)/2023

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

Bucharest
2023

CONTENT

CYBERINTELLIGENCE

FROM INTELLIGENCE GATHERING TO CYBER THREAT DETECTION

Antonio VILLALÓN-HUERTA[*]
Ismael RIPOLL-RIPOLL[*]
Héctor MARCO-GISBERT[*]

Abstract:
Intelligence plays a key role in the detection and neutralisation of threat actors in cyberspace, particularly when dealing with advanced ones. However, the relationship between intelligence and the final detection capabilities is not well–defined in most cases. Even the role of information gathering disciplines, which are the basis of intelligence and therefore of cyber intelligence, is confusing and not consensual between authors. In this work we contextualize intelligence gathering disciplines in the cyber intelligence arena. We discuss the role of all of these disciplines in the characterization of advanced threat actors, from the strategic to the tactical views. Once characterization has been performed, we analyse the detection capabilities that intelligence provides, in the form of indicators of compromise, both low–level and behavioural ones. Following this approach, in this work we are defining the road from initial intelligence gathering to threat detection.

Keywords: *Intelligence, Cyber Intelligence, CYBINT, Tactics and Techniques, TTP, Indicators of Compromise*.

Introduction

Advanced Threat Actors are actors with high capabilities (technical, economic, etc.) that perform hostile activities through cyberspace. The threat from these actors is a real fact, as being targeted

[*] Chief Security Officer at S2 Grupo. Valencia, Spain; email: antonio.villalon@s2grupo.es
[*] Assistant Professor at the Department of Computing Engineering, Universitat Politècnica de València, Camino de Vera s/n, 46022 Valencia, Spain; email: iripoll@disca.upv.es
[*] Associate professor and cybersecurity researcher at Department of Computing Engineering, Universitat Politècnica de València, Camino de Vera s/n, 46022 Valencia, Spain; email: hecmargi@disca.upv.es

by one of them is non-discriminatory: every organization with valuable information, every critical operator for basic services and even every single citizen is a potential target. We face two types of advanced threat actors: those linked to nation–states and those linked to criminal gangs. Both of them have the budget, the intent, the time and the capability to perform hostile activities. This is a growing trend that is expected to increase for years: beyond classical operations related to espionage, attack or crime, cyberspace provides threat actors enormous benefits such as accessibility, plausible deniability or geographical offshoring.

Intelligence plays a key role in the detection of hostile cyberspace operations. However, this role is not always well–defined, as in many cases threat analysts focus on pure threat detection mechanisms, not considering the intelligence process nor the threat's features in this detection. As an example, the main *de facto* standard for the characterization of advanced threat actors, MITRE ATT&CK, presents different concept problems in tactics such as Reconnaissance, where elements such as information needs, intelligence gathering and reconnaissance techniques are wrongly mixed.

In this work, we discuss the process that enables threat detection from intelligence gathering. Intelligence as a product turns information gathered, through multiple disciplines, into strategic, operational and tactical intelligence. This intelligence enables the characterization of threat actors, i.e., the identification of the main features of a threat actor or even of a particular operation. Finally, some of these features, the observable ones, are expressed as indicators of compromise, pieces of information that can be used to identify a potentially compromised system.

The main contributions of this work are as follows:

- To discuss the role of intelligence gathering disciplines in cyber intelligence.
- To define the mandatory road map to turn raw information into actionable intelligence.
- To define the main features for the characterization of threat actors.
- To discuss threat actors' detection through observable features.

The rest of the paper is organized as follows. In the next section we present the main concepts related to intelligence, intelligence gathering disciplines and cyber intelligence, later discussed in this work. Next, we discuss the process from intelligence to threat detection. Starting with intelligence gathering, we delve into threat actors' characterization to end with threat actor's detection, which is the final goal of the intelligence: enabling the detection and response capabilities to neutralize the threat. Finally, in the last section we present the main conclusions of our work.

Background

Intelligence. NATO (Office, 2018) defines intelligence as "the product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision–makers". The same work also defines the intelligence cycle as "the sequence of activities whereby information is obtained, assembled, converted into intelligence and made available to users". The intelligence cycle as exposed in Staff (2013) is shown in figure one (fig. 1). There are different versions of this cycle, and their alternatives and key differences have been discussed in different works (Hulnick, 2006; Phythian, 2013; Mocanu, 2015) provides key differences between relevant models. However, we can summarize its approach by considering the following five steps:

- Direction. "Determination of intelligence requirements, planning the collection effort, issuance of orders and requests to collection agencies and maintenance of a continuous check on the productivity of such agencies."
- Collection. "The exploitation of sources by collection agencies and the delivery of the data obtained to the appropriate processing unit for use in the production of intelligence."
- Processing. "The conversion of data into usable information suitable for analysis."
- Analysis. "Integration, evaluation, interpretation etc. of information to turn it into intelligence."

- Dissemination. "The timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it."

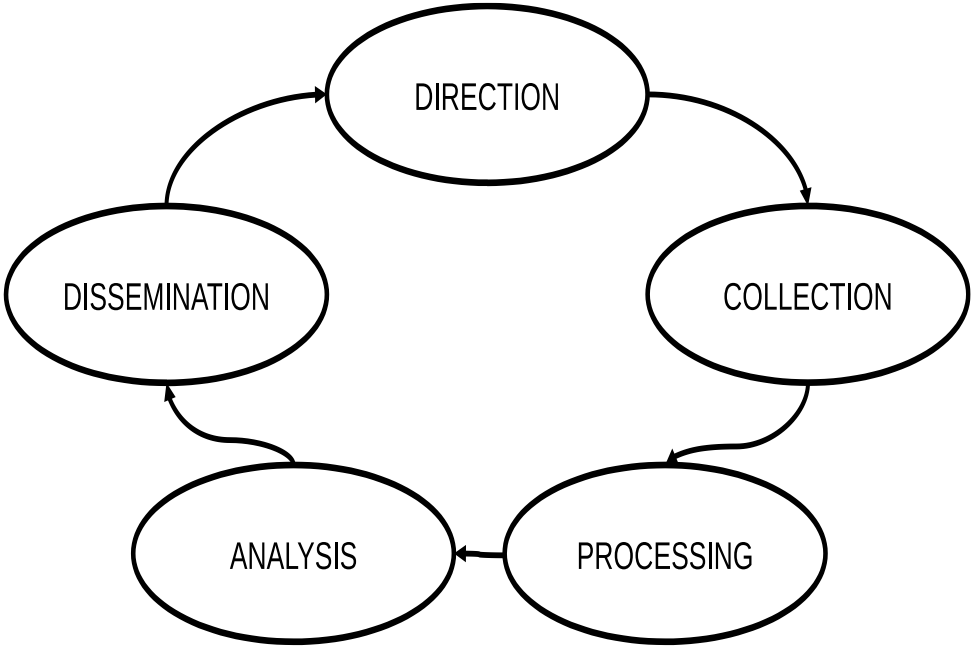

Figure 1: Intelligence Cycle (Source: Authors' view)[1]

Ackoff (1989) and Liew (2007 and 2013) provide precise definitions of data, information and intelligence. Madureira et al. (2021) identify intelligence as a product as one of the five dimensions of intelligence; it is the final result of the intelligence cycle (Bimfort, 2007). The intelligence cycle is a simple explanation of a complex process; intelligence as a process is is also a key dimension of intelligence (Madureira et al., 2021). In Villalón-Huerta et al. (2022) we stated that it starts "when someone (an authority, a government, etc.) has particular intelligence needs in order to make the best decision about a particular subject". When dealing with government intelligence, this subject is usually relevant for national

[1] Authors' view previously published in Villalón-Huerta et al. (2022).

security. At this point the cycle starts first by identifying the requirements and planning the acquisition of the information to be processed and analyzed, in order to generate intelligence.

"Once planned, the next stage is to acquire information, and this acquisition can be performed through different intelligence collection disciplines" (Boury-Brisset et al., 2011) commonly referred as "the INTs" (Villalón-Huerta et al., 2022); "the essential elements of these INTs are not formally defined" (Clark and Oleson, 2018), nor are them consensual "between authors, but they define the families of sources the information can be gathered from: a simple public website, a satellite, an intercepted artifact, a mole etc." These intelligence collection disciplines are discussed in next section.

Once data has been gathered, processing turns it into "a form suitable for the production of finished intelligence" (Richelson, 2018). This stage includes tasks such as decryption, translation or data conversion. As a part of the cycle, it is mandatory to the next one: analysis, in which the intelligence, the final product, is generated. This analysis must include the information gathered and processed no matter which collection discipline it comes from. In this sense, we can refer to all–source intelligence, defined by Army (2004) as "the intelligence products, organizations, and activities that incorporate all sources of information and intelligence, including open-source information, in the production of intelligence."

"Finally, once the intelligence as a product has been generated, it is delivered to and used by the customer, the entity which had the information needs stated before, in a suitable form for its use and by a variety of means. This product will be used to help the decision-making process and, possibly, to start a new iteration of the intelligence cycle." (Villalón-Huerta et al., 2022) After the product is disseminated and consumed, different intelligence needs, and additional information or new tasks can be arised (Bartes, 2013).

Intelligence gathering disciplines. As stated before, intelligence collection disciplines are not consensual between authors, so they motivate different discussions. There are five commonly accepted disciplines by the US Intelligence Community (Lowenthal, 2019;

Lowenthal and Clark, 2016; Phythian, 2013; Clark and Oleson, 2016): geospatial (formerly imagery) intelligence (GEOINT), signals intelligence (SIGINT), measurement and signatures intelligence (MASINT) – which includes technical intelligence or TECHINT –, human intelligence (HUMINT) and open source intelligence (OSINT).

"IMINT is defined as the technical, geographic, and intelligence derived through the interpretation or analysis of imagery and collateral material" (Cardillo, 2018), and it is considered inside GEOINT in some works (Randol, 2010; Clark and Oleson, 2018), although it is also considered as an independent discipline in many others (Goldman, 2015; Carlisle, 2015). Most references seem to consider GEOINT as the integration of imagery, IMINT, and geospatial information (Defense, 2017; Cardillo, 2018), so we will deal with GEOINT as a global discipline comprising IMINT. It is important to note that there is no collection system that gathers data from GEOINT (Clark, 2013): geospatial information is collected via IMINT, OSINT, SIGINT, HUMINT or MASINT.

The role of TECHINT, intelligence gathered from the collection, processing, analysis and exploitation of data and information pertaining to foreign equipment and materiel (Bautista, 2018), is much more discussed. It is considered inside MASINT by the references which identify only five main disciplines and by specific military works (US Air Force, 2021; North Atlantic Treaty Organization, 2022). However, it is considered a discipline by itself in different references (Carlisle, 2015; D. E. Johnson and Howard, 2012). Other works identify TECHINT as all intelligence gathered from technical sources – vs. human sources –, (Guliyev, 2010; Shulsky and Schmitt, 2002; Crosston and Valli, 2017; L. K. Johnson, 2017). Finally, some authors, such as (Herman, 1996), differentiate between main and smaller sources for intelligence gathering disciplines. These smaller sources (for example, NUCINT, Nuclear Intelligence) are referred as secondary sources, as the term "small" does not properly describe the meaning of this category. Saunders (2000) makes a discussion about those disciplines and their consideration. In addition to these differences, there have been also some efforts to add new intelligence collection disciplines to the list, such as those proposals in (Taylor, 2007; Faint, 2011; Arslan and Yanık, 2015), generating even more confusion into the community.

In this work we will not enter into the discussion about which disciplines have to be considered: we will simply deal with the five generally–accepted disciplines. We will include TECHINT inside the MASINT discipline and, in the same way, we will include IMINT inside GEOINT, in order to highlight that imagery intelligence plays a key role in the cyber battle space (much more than GEOINT, as cyber is a domain of conflict not directly related to GEO in many cases). In summary, we are considering the following five disciplines, without detailing subcategories for the purpose of this work:

- Human Intelligence (HUMINT). Intelligence collected and provided from human sources (Staff, 2013).
- Geospatial Intelligence (GEOINT). Intelligence gathered from geospatial data through the application of geospatial techniques and by skilled interpretation, in which the location and movement of activities, events, features and people play a key role (Council, Committee, et al. 2006).
- Measurement and Signature Intelligence (MASINT). Technically derived intelligence that "enables detection, location, tracking, identification and description of unique characteristics of fixed and dynamic target sources" (Lowenthal and Clark, 2015). As stated, it includes TECHINT, intelligence gathered "from the collection, processing, analysis and exploitation of data and information pertaining to foreign equipment and materiel" (Bautista, 2018).
- Signals Intelligence (SIGINT). Intelligence produced by "exploiting foreign communications systems and non-communications emitters" (Staff, 2013), which comprises three subcategories: communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT).
- Open-Source Intelligence (OSINT). Intelligence gathered from publicly available information that is "collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement" (Williams and Blum, 2018).

Cyber intelligence

Cyber Intelligence, CYINT or CYBINT, is intelligence related to cyberspace, a concept that has no single definition. While HUMINT is considered as intelligence from human sources, CYBINT cannot be the equivalent, intelligence from cyberspace; the term is generally "used to convey the idea of widely scoped and better qualified knowledge of actual or potential events regarding cyberspace that may endanger an organization" (Bonfanti, 2018). CYBINT cannot be considered as a collection discipline, but an analytic one: this is, with its focus on the analysis stage of the intelligence cycle, relying on data collected from the gathering disciplines stated before (Alsmadi, 2019; Seedyk, 2018): SIGINT, HUMINT, MASINT, OSINT and GEOINT.

In 2011 Intelligence and National Security Alliance (INSA) published (Fast et al., 2011) the first formal and high-level approach to the "emerging discipline" of CYBINT, providing a "framework to approach the development of intelligence in the cyber domain" and stating it as a new discipline in the US Intelligence Community, but without providing an accurate definition of the term. The same year some authors stated the earliest definitions of cyber intelligence, referred to it as "the process of obtaining specific types of valuable information and knowledge through the Internet" (Petratos, 2011) or "collecting, relating, analysing, and reporting information about a topic, an organization or a person, from sources available on the internet and other open sources" (Tekes, 2011). These initial definitions make a clear reference to intelligence gathered from Internet, and have been superseded during the decade with more accurate terms that better fit the concept that today we have of the term.

With the early concept of intelligence from Internet, in 2012 (Hurley, 2012) started a discussion about what CYBINT is, differentiating "from" and "for" cyber, "depending on the scope of the information gathering activities, the means employed to carry them out and their final goal". Bonfanti (2018) states that intelligence "from" is "knowledge produced through the analysis of any valuable information collected within or through cyberspace", while intelligence "for" refers to capabilities to enable cyberspace operations regardless of the source, method or medium: this is, different collection disciplines providing valuable intelligence to these operations.

In 2013, Bamford et al. stated that CYBINT "should not be limited to an understanding of network operations and activities, but should include the collection and analysis of information that produces timely reporting, with context and relevance to a supported decision maker" (Bamford et al., 2013). Although yet undefined, what was clear is that the term refers to a "multifaceted approach to framing, thinking about, and reacting to cyber adversarial activity", not only regarding intelligence from cyber space.

Although still nowadays there is no consensus about a formal CYBINT definition (relevant discussions can be found at Kandiko, 2018; Seedyk, 2018; Bonfanti, 2018), one useful and simple approach was proposed in (Townsend et al., 2013), which states CYBINT as the acquisition and analysis of information "to identify, track, and predict cyber capabilities, intentions, and activities that offer courses" of action to enhance decision making. This definition fits well in what is usually understood as CYBINT by security product vendors and services providers, as the product derived from the analytic discipline, focusing in cyber intelligence for cyberspace but also including intelligence gathered from cyberspace, as long as it is useful for cyber activities. In fact, when we refer to intelligence gathered from cyberspace to satisfy information needs outside this battlefield, we could simply refer to classical collection disciplines. For the purpose of this work, we will be using this definition.

In addition to CYBINT, a term that is usually used among the information security community is Cyber Threat Intelligence, or CTI, first defined (McMillan, 2013) as "evidence–based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard." In other words, CTI focuses (Coats, 2019) on all source intelligence on threats: programs, intentions, capabilities, research and development, tactics, targets, operational activities and indicators, potential impacts, infrastructure and data, characterization and structures. The term is used without the cyber prefix – this is, Threat Intelligence or TI –, and its goal is (Conti et al., 2018) "to help organizations in recognizing the indicators of cyber attacks, extracting information

about the attack methods, and consequently responding to the attack accurately and in a timely manner." CTI can be considered as a subset of CYBINT: CYBINT includes CTI, but CTI does not represent all of CYBINT (Ettinger, 2019). While CTI focuses on the single analysis of threats, cyber intelligence includes this analysis, but also analysis of areas such as geopolitics, military or diplomacy; CTI, from its definition to its goal or its components, focuses on threats, not in their external context.

In intelligence, including CYBINT and CTI, it is possible to identify different levels to deal with; in fact, it is possible to identify these levels in all intelligence–related activities. Each of these levels refers to intelligence with a specific goal, time of life, type of product etc. They are defined as follows (Bamford et al., 2013; Joint Chiefs of Staff, 2010; Abu et al., 2018):

- Strategic. Level at which an actor determines global strategic security objectives and guidance, and develops and uses resources to achieve these objectives. In the cyber domain, strategic intelligence provides knowledge to understand threats and risks at a senior management level: main actors and their motivations, victims and their relations, links to geopolitical events, etc. The final product is usually in the form of written reports with a long lifetime and a non–technical approach, about who and why.
- Operational. "Level at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas." (Bamford et al., 2013; Joint Chiefs of Staff, 2010; Abu et al., 2018) In the cyber domain, operational intelligence provides knowledge about the context and trends of past incidents (Meeuwenberg, 2017): tactics, techniques, patterns, actor profiles, etc. The final product is in the form of short written reports with a medium lifetime, about how and where.
- Tactical. "Level at which battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces." (Bamford et al. 2013; Joint Chiefs of Staff, 2010; Abu et al. 2018) This is the most basic form of intelligence, and in the cyber domain it provides knowledge about

the identification of threats targeting the infrastructure in the form of hashes, IP addresses, domains or detection rules. The final product is in the form of atomic indicators in a machine–readable format, such as Yara rules, IDS signatures or blacklists, suitable to load them in different security devices. Tactical intelligence has a short lifetime and tries to answer what is happening or what is to happen in short term.

These levels, and their associated products, are shown in figure 2. Other works (Sari, 2018; Mutemwa et al., 2017; Leszczyna and Wróbel, 2019) change the definitions and layers of tactical and operational levels of intelligence, while studies such as (Noor et al., 2018) include a fourth level, called technical, at the lowest part of the heap.

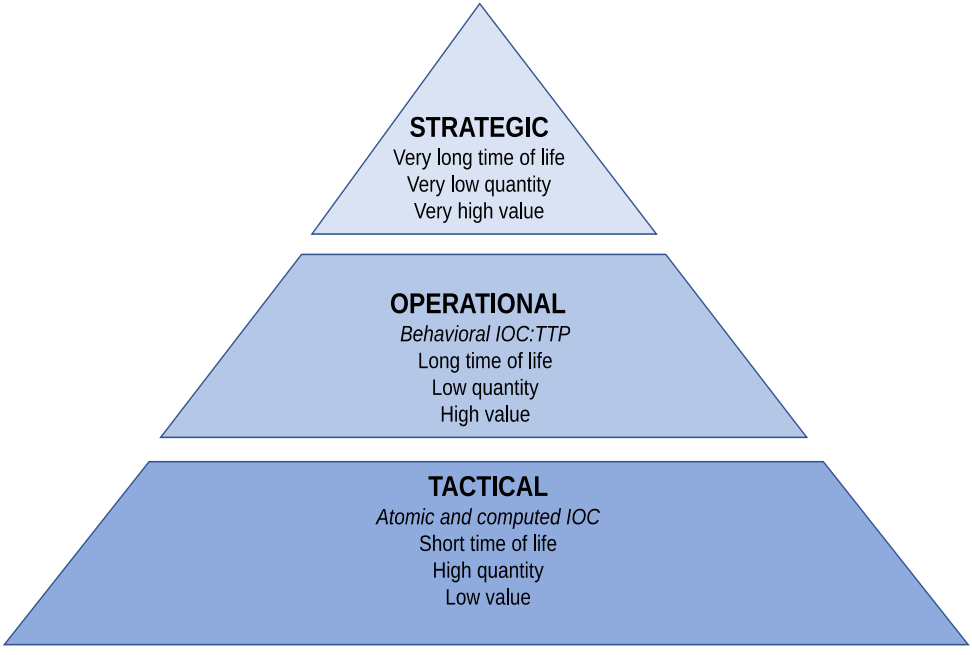

Figure 2: Intelligence levels (Source: Authors' view)[2]

[2] Authors' view previously published in Villalón-Huerta et al. (2022).

From intelligence gathering to threat detection

In this section we discuss the process that turns information into actionable intelligence. We divide it into three parts. The first one gathers information to identify the main features of an operation. Second part refers the characterization of threat actors and their operations, through the previously generated intelligence. Finally, third part is related to threat detection and specifies, when possible, the extracted features to turn them into actionable intelligence. This process is summarized in figure three (fig. 3).

The detection and the later analysis of an offensive cyberspace operation can be performed through all of the intelligence gathering disciplines we have exposed in section "Intelligence gathering disciplines", from SIGINT to OSINT. All these disciplines are relevant to identify features of an operation, from the strategical to the tactical ones. In this way, they all are helpful to characterize the operation. Through this characterization, they all allow the detection of hostile activities, especially through operational and tactical intelligence. Both intelligence types are specified as actionable indicators of compromise (low level ones, atomic and computed, and behavioural ones, tactics and techniques).

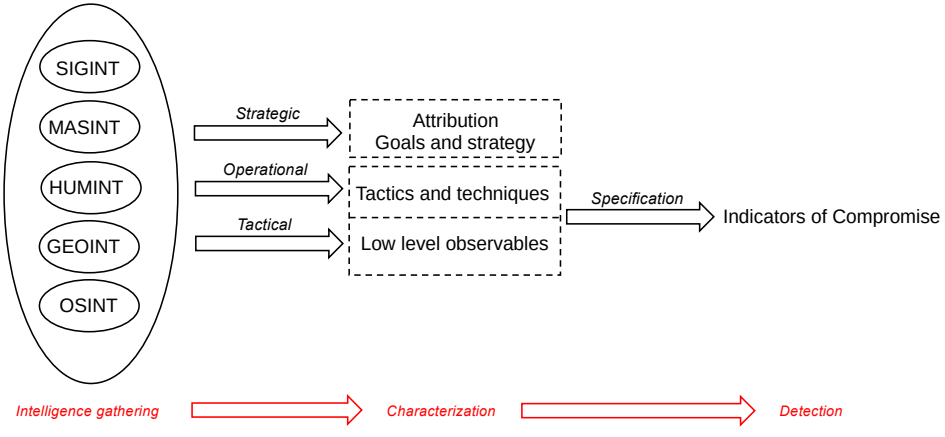

Figure 3: The role of information gathering disciplines in threat detection (Source: Authors' view)

Intelligence gathering

Although intelligence gathering disciplines are relevant for cyber intelligence, not all of them have the same weight on the detection equation. The main intelligence gathering discipline in cyber intelligence is SIGINT, recognized as the primary driver for operations within the cyberspace operating environment (Franz et al. 2019; Oakley, 2019). In fact, many of the services or units historically focused on SIGINT activities are nowadays tasked with cyber operations, such as US National Security Agency, NSA, (Loleski, 2019; Kris, 2021), UK Government Communications Headquarters, GCHQ, (Aldrich, 2021) or Israel Defence Forces Unit 8200 (Cordey, 2019). Cyberspace has become the main way to communicate, and interception and gathering of network signals muddies the traditional notion of SIGINT (Richards, 2014). Most detection approaches are based nowadays on SIGINT capabilities: this is, on the detection of anomalous activities in one's own infrastructure, through the monitoring of systems and networks. SIGINT provides tactics, techniques and procedures of implants communicating laterally and externally (command and control and exfiltration), as well as the relevant atomic indicators regarding these communications.

MASINT, specifically TECHINT, plays also a key role in the cyberspace domain. In the kinetic sphere, TECHINT refers to the collection and analysis of adversary's equipment and materiel; in cyberspace, media and software, particularly malware (Fanelli, 2015), are the equivalent to this equipment and materiel. Through disciplines such as malware analysis and forensic analysis, TECHINT provides relevant information not only in the tactical level, but also in the operational and strategical, from the most technical indicators of compromise to aspects such as an adversary's budget or interest in its target (Richmond, 2011; Porche III et al. 2011).

HUMINT remains fundamental for understanding threats' capabilities and intentions (Gioe, 2017) in cyberspace, not being replaced by any of the other acquisition disciplines. While these ones provide vast volumes of intelligence, human sources provide excellent – not vast, but excellent – information about adversaries. It is particularly relevant the interest of different services in deploying cover HUMINT capabilities targeting units in hostile services or telecommunications

industries – GCHQ Human Operations Team, HOT, is an example (Duvenage and Solms, 2014). In addition, overt capabilities among interest groups to get effective information sharing regarding cyber capabilities, interests or activities of potential adversaries is also a particularly relevant element for HUMINT approaches (Brown, Gommers, and Serrano, 2015). An example of an overt cyber intelligence sharing effort is the European Government CERT (EGC) group (Ilves et al., 2016).

OSINT is also a big player in cyber intelligence. Although it is difficult to identify very targeted attacks through open-source intelligence, OSINT provides useful information about general trends that could be relevant to intelligence analysis. In fact, most cyber intelligence shared nowadays is on the form of threat intelligence feeds and private intelligence reports regarding advanced threat actors; both of these examples must be considered OSINT. As in intelligence not related to cyberspace, from an analytic perspective one of the main problems to face in OSINT is the reliability of the source where information is gathered from (Steele, 2007; Gong et al., 2018). Although different analysis on the quality of intelligence feeds is available (Meier et al., 2018; Li et al., 2019; Griffioen et al., 2020), we identify this as a relevant problem in cyber intelligence. In addition to threat intelligence feeds, the monitoring, analysis and research of information coming from the Internet (Lande and Shnurko-Tabakova, 2019) is a must, so a global monitoring schema must include open-source monitoring for the tracking of adversarial capabilities: this is, OSINT.

Finally, GEOINT related to cyber is clear in military operations: Army (2010) states that "cyberspace can be viewed as three layers (physical, logical, and social) made up of five components (geographic, physical network, logical network, cyber persona, and persona)." The lowest of these three layers, the physical one, includes the geographic component, referring to the physical location of elements of the network and denoting a physical aspect tied to the rest of components. It is commonly accepted that information cannot exist without a physical infrastructure to support it. Cyberspace has been created as a domain by this infrastructure and has a relevant geospatial component (Taneski et al., 2019). For this reason, there have been some efforts to "visualize"

cyber using intelligence fusion and GEOINT techniques, trying to connect the "bits and the bytes" with the "bricks and mortar" (Price, 2014). To ensure this connection it is mandatory to geolocate network activity, tracking actions in both network time and space (Franz et al., 2019) towards cyber-physical spatialization in order to detect hostile operations. Relevant geolocations have been shown during armed conflicts (Higgins 2016; McCrory, 2020), as examples of all-source intelligence.

As we have stated before, all information gathering disciplines are relevant for the characterization, and further detection and analysis, of hostile activities. Although GEOINT is the less exploited one, all of them can provide strategical, operational and tactical intelligence. For this reason, an accurate security approach must consider all of them, not only for pure detection but for the whole analysis and modelling of the threat actors' activities and interests. In fact, the mix of different intelligence acquisition disciplines is common in real world operations (Oakley, 2019): we return to the all–source intelligence concept. All of these disciplines provide the mandatory intelligence for the characterization of threat actors and their activities, thus all of them can enable the detection of hostile activities in our infrastructures, as we have summarized in figure three (fig. 3).

Threat characterization

The characterization of threat actors is the recognition and analysis of its features, in order to identify their attribution, goals and strategies, tactics and techniques and tools and artifacts. Although this characterization can be performed through all the intelligence gathering disciplines, SIGINT and TECHINT are the most relevant ones in most cases, as the characterization usually starts by direct observables that are turned into indicators of compromise. However, to discuss the whole characterization of threat actors, we must consider both direct observables and non–observable elements, such as goals, strategy and even attribution. As these ones are not directly seen in an operation, they must be inferred from an intelligence analysis, apart from the purely technical aspects of the operation. This analysis, outside of the scope of this work, will infer, with an associated probability, why a threat actor is

conducting a hostile operation against a particular target. The identification of goals, strategies and attribution provides valuable information to establish tailored security countermeasures to face specific threat actors.

In table one we summarize the main families of features regarding threat actors. We must differentiate between observable features (those that can be directly seen on an operation) and non–observables ones (those that are not directly seen, so they must be inferred or acquired by external intelligence). Low–level observables are linked to tactical intelligence and tactics, techniques and procedures (TTP) are linked to operational intelligence. Both of them can be expressed in the form of indicators of compromise, as we will discuss in next section. On the other hand, non–observables are mostly linked to strategical intelligence. It is important to highlight that when we refer to observable features, not all of them can be observed through cyberspace, but they can be gathered through different intelligence gathering disciplines. As we have stated, all of them are relevant for an accurate characterization of a threat actor, although strategical intelligence is rarely actionable.

Table 1: Threat actors' features (Source: Authors' view)

Non–observables	Attribution
	Goals and strategy
Observables	TTP
	Low–level indicators

Threat characterization starts with low–level observables and ends with the attribution, one of the main relevant problems that threat intelligence analysts face nowadays. All of the discussed features are important to the whole characterization of a threat actor, from its arsenal to its interests. However, we defend that the characterization of advanced threat actors must be mainly approached by the analysis of their tactics and techniques. They are the most valuable observables in the context of a cyberspace operation. This value is linked to the fact that lower level observables, such as atomic indicators of compromise, or even tools or artifacts, are easily modified by an actor, so their value is

limited. On the other hand, characteristics such as goals and strategies, or even attribution, are not direct observables in a hostile operation and in most cases, they must be inferred from the operational and tactical levels, where observables are usually found. In table 2 a brief description of TTP is provided.

Table 2: Threat actors' features (Source: Authors' view)

Tactics	The employment and ordered arrangement of forces in relation to each other.
Techniques	Non–prescriptive ways or methods used to perform missions, functions, or tasks.
Procedures	Standard, detailed steps that prescribe how to perform specific tasks.

Tactics represent what a threat actor is doing at the highest level of description, to accomplish a certain mission. In literature, they have been structured in frameworks such as MITRE ATT&CK (Strom et al., 2017; Xiong et al., 2022), in different kill–chain models such as the Cyber Kill Chain (Hutchins et al. 2011) and in models such as The Cyber Diamond Model (Al-Mohannadi et al., 2016). Techniques specify how a tactic is implemented. From an intelligence point of view, their value is very high for the characterization of a threat actor, as well as for its detection. Finally, procedures are particular implementations of a given technique, linked to specific threat actors of even operators. Being so particular is not useful for the detection of an offensive cyberspace operation, as in general terms they do not provide relevant information that is not provided by their superior techniques, so they are out of the scope of this work.

Tactics and techniques, operational intelligence, describe the modus operandi of a threat actor and they are a key element for its characterization, as they are not easily modified. To be effective, tactics and techniques must be represented in a machine-readable format that can be loaded into security devices and automatically provide accurate results. We consider this is one of the biggest challenges we must face today. Common formats and languages have been developed in order to allow this specification and the sharing of tactics and techniques in the

form of actionable intelligence. However, the lack of a common standard is a current problem, as most of these formats are vendor–dependent. Without such a common standard, actionable intelligence is based nowadays mostly in atomic and computed indicators of compromise, easy to consume but with a very short time of life. This fact opens a window of opportunity for threat actors, as low–level indicators of compromise are easy to evade.

Threat detection

Once threats have been characterized by the identification of their main features, these features must be exploited to detect hostile activities in a compromised infrastructure. This detection is carried through Indicators of Compromise (IOC), the specification of observable features in order to search their presence in an infrastructure. IOC are defined (Harrington, 2013) as a piece of "information that can be used to identify a potentially compromised system". They play a key role in Cyber Threat Intelligence, as they enable and accelerate the detection of hostile activities in targeted infrastructures. IOC allow the specification both of the usage of "technological capabilities, such as tools or artifacts, and of the tactics, techniques and procedures developed by threat actors."

IOC can be classified into three categories (Cloppert, 2009; Hutchins et al., 2011): atomic, computed and behavioural. The first two types are considered low–level IOC and they are linked to tactical intelligence. Examples of such indicators are IP addresses, file hashes or malicious domain names. Behavioural indicators represent the tactics and techniques of threat actors, and they are linked to operational intelligence. All of them are relevant to detect compromises, but tactical intelligence has a shorter lifetime than operational intelligence, and it can also be more easily evaded, so it is less useful in general terms.

Being SIGINT, the main information gathering discipline for the detection of hostile activities, most of the current approaches to this detection rely on the specification and sharing of atomic and computed indicators of compromise. As stated, these indicators have a limited value and time of life, as they are easily modified by threat actors. For an effective detection capability, it is mandatory to work at the operational intelligence level, this is, the one related to tactics, techniques and

procedures: behavioural indicators of compromise. For this reason, we defend that the specification of tactics and techniques is a key element for threat detection.

However, it is known that not all detection is based on indicators of compromise. In this sense, threat hunting is defined (Shu et al., 2018) as "the process of proactively and iteratively formulating and validating threat hypotheses based on security relevant observations and domain knowledge." Threat hunters acquire relevant information from the infrastructure, such as network traffic or endpoint activity, and they analyse this information to formulate and validate hypotheses. This process is an intelligence activity, specifically a SIGINT one. It gathers signals information, analyse it to identify hypotheses, in the form of observables, both low–level and behavioural ones, and validates these hypotheses. If they are valid ones, observables are specified and their search is automated.

In addition to the exploitation of indicators of compromise or threat hunting activities, intelligence sharing, as a dissemination approach, must also be particularly considered in an effective detection scheme. Intelligence sharing, from strategical to tactical, is a must for threat detection, as in most cases we face global threats and there is a consensus that no intelligence actor can successfully act alone (Kalkman and Wieskamp, 2019). Collaboration between organizations is a key point to prevent, to detect and to neutralize threats. As an example, we can refer to formalized CERT groups such as FIRST or TF-CSIRT (Kossakowski, 2019), US ISAC (McCarthy et al., 2014) or UK WARP (Proctor, 2011). Intelligence must be shared among a community, a group of trusted stakeholders who work together to address shared threats or vulnerabilities (Willis, 2012), usually with common interests; the formalized groups referenced below are examples of communities. Inside each type of community, elements such as the trust model or the sharing intelligence policy define how intelligence is shared.

Information shared must meet three requirements to be considered valid threat intelligence (Dalziel, 2014): it must be relevant, actionable and valuable. As we have stated, most shared intelligence is in the form of low-level data (Pawlinski et al., 2014), especially atomic indicators (Sauerwein et al., 2017): this is, a very tactical approach that

focuses on elements such as malicious IP addresses, DNS domains or URL. Operational and strategical intelligence are much less shared, although they are more valuable than tactical one.

Finally, to share intelligence, it is mandatory to establish exchange mechanisms over a technological platform that can be deployed in many forms such as centralized or peer to peer. Sauerwein et al. (2017) states that there is no common definition of threat intelligence sharing platforms, being most of them focused on the exchange of tactical intelligence in STIX format. In fact, what we call threat intelligence sharing platforms, such as MISP, are focused on this kind of tactical intelligence, but are not usually suitable for strategic intelligence sharing.

Conclusions

As we have stated in this work, intelligence plays a key role in the detection of offensive cyberspace operations. However, it is not always clear how intelligence must be applied to the characterization of advanced threat actors and to the detection of their operations. In this paper we have discussed the process that turns raw information into valuable actionable intelligence to detect hostile operations. Through the application of all intelligence gathering disciplines, information is acquired, processed and analysed to identify the main features of threat actors or of their operations. This intelligence can be exploited at strategical, operational and tactical levels: all of them are relevant in the cyberspace arena, and all of them can be obtained from each of the intelligence gathering disciplines.

The identified features that characterize a threat actor can be divided into observable and non–observable ones. As their name implies, observable features can be directly seen on the targeted infrastructure, while non–observable ones must be inferred. Observable features are particularly relevant for the detection of advanced threat actors. They can be expressed as indicators of compromise, defined as pieces of information that can be used to identify a potentially compromised system. These indicators are actionable intelligence that enables and accelerates the detection of hostile activities in targeted infrastructures. Particularly, operational intelligence, in the form of behavioural

indicators of compromise, is a must for an accurate detection capability. In this way, the path from raw information to actionable intelligence is defined. We defend that threat detection must be based on the result of intelligence acquisition and analysis, and on the further characterization of advanced threat actors. With this structured approach, intelligence-driven threat detection can be performed and, which is most important, enhanced over time.

Reference:

1. Abu, Md Sahrom, Siti Rahayu Selamat, Aswami Ariffin, and Robiah Yusof. (2018). "Cyber Threat Intelligence – Issue and Challenges." *Indonesian Journal of Electrical Engineering and Computer Science* 10 (1): 371-379.

2. Ackoff, R. L. (1989). From data to wisdom. *Journal of applied systems analysis*, 16(1), 3-9.

3. Aldrich, Richard J. (2021). "From Sigint to Cyber: A Hundred Years of Britain's Biggest Intelligence Agency." *Intelligence and National Security,* 36 (6): 910-917.

4. Alsmadi, Izzat. (2019). "Cyber Intelligence Analysis." In *The NICE Cyber Security Framework*, 91-134. Springer.

5. Al-Mohannadi, H., Mirza, Q., Namanya, A., Awan, I., Cullen, A., & Disso, J. (2016, August). Cyber-attack modeling analysis techniques: An overview. In 2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW): 69-76.

6. Army, US. (2004). "Field Manual 2-0 Intelligence." US Department of the Army.

7. Army, US. (2010). "TRADOC Pamphlet 525-7-8. Cyberspace Operations Concept Capability Plan 2016-2028." United States Army.

8. Arslan, C, and M Yanık. (2015). "A New Discipline of Intelligence: Social Media." *Military and Security Studies*, 69.

9. Bamford, George, John Felker, and Troy Mattern. (2013). "Operational Levels of Cyber Intelligence." *Cyber Intelligence Task Force, Intelligence and National Security Alliance*.

10. Bartes, F. (2013). Five-phase model of the intelligence cycle of competitive intelligence. Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis, 61(2), 283-288.

11. Bautista, Wilson. (2018). *Practical Cyber Intelligence: How Action-Based Intelligence Can Be an Effective Response to Incidents*. Packt Publishing Ltd.

12. Bimfort, M. T. (2007). A definition of intelligence. Studies in Intelligence, 2.

13. Bonfanti, Matteo E. (2018). "Cyber Intelligence: In Pursuit of a Better Understanding for an Emerging Practice." *Cyber, Intelligence, and Security* 2 (1): 105-121.

14. Villalón-Huerta, A., Ripoll-Ripoll, I, and Marco-Gisbert, H. (2022). "Key Requirements for the Detection and Sharing of Behavioral Indicators of Compromise", *Electronics*, Volume 11, Issue 3, 2022, 416.

15. Boury-Brisset, Anne-Claire, Anissa Frini, and Réjean Lebrun. (2011). "All-Source Information Management and Integration for Improved Collective Intelligence Production." Defence Research; Development Canada Valcartier (Quebec).

16. Brown, Sarah, Joep Gommers, and Oscar Serrano. (2015). "From Cyber Security Information Sharing to Threat Management." In *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, 43-49.

17. Cardillo, Robert. (2018). "Geospatial Intelligence (GEOINT) Basic Doctrine." National System for Geospatial Intelligence.

18. Carlisle, Rodney. (2015). *Encyclopedia of Intelligence and Counterintelligence*. Routledge.

19. Clark, Robert M. 2013. "Perspectives on Intelligence Collection." *Journal of U.S. Intelligence Studies* 20 (2): 47-53.

20. Clark, Robert M., and Peter C. Oleson. (2016). "Intelligence in Public Literature." *Studies in Intelligence* 60 (1): 81–96.

21. Clark, Robert M., and Peter C. Oleson. (2018). "Cyber Intelligence." *Journal of U.S. Intelligence Studies* 24 (3): 11-23.

22. Cloppert, Mike. (2009). "Security Intelligence: Attacking the Cyber Kill Chain." *SANS Computer Forensics* 26.

23. Coats, Daniel R. (2019). "National Intelligence Strategy of the United States of America 2019." *Office of the Director of National Intelligence, Washington, DC*.

24. Conti, Mauro, Tooska Dargahi, and Ali Dehghantanha. (2018). "Cyber Threat Intelligence: Challenges and Opportunities." In *Cyber Threat Intelligence*, 1-6. Springer.

25. Cordey, Sean. (2019). "The Israeli Unit 8200–an OSINT-Based Study: Trend Analysis." ETH Zurich.

26. Council, National Research, Mapping Science Committee, et al. (2006). *Priorities for GEOINT Research at the National Geospatial-Intelligence Agency*. National Academies Press.

27. Crosston, Matthew, and Frank Valli. (2017). "An Intelligence Civil War: HUMINT Vs. TECHINT." *Cyber, Intelligence, and Security* 1 (1): 67-82.

28. Dalziel, Henry. (2014). *How to Define and Build an Effective Cyber Threat Intelligence Capability*. Syngress.

29. Defense, US Department of. (2017). "Joint Publication 2-03. Geospatial Intelligence in Joint Operations." US Department of Defense.

30. Duvenage, Petrus, and Sebastian von Solms. (2014). "Putting Counterintelligence in Cyber Counterintelligence: Back to the Future." In *13th European Conference on Cyber Warfare and Security ECCWS-2014 the University of Piraeus Piraeus, Greece*, 70.

31. Ettinger, Jared. (2019). "Cyber Intelligence Tradecraft Report. The State of Cyber Intelligence Practices in the United States." Carnegie–Mellon University. Software Engineering Institute.

32. Faint, Charles D. (2011). "Exploitation Intelligence (EXINT) a New Intelligence Discipline?". *American Intelligence Journal* 29 (1): 65-69.

33. Fanelli, R. (2015). "On the Role of Malware Analysis for Technical Intelligence in Active Cyber Defense." *Journal of Information Warfare* 14 (2): 69-81.

34. Fast, Barbara, Michael Johnson, and Dick Schaeffer. (2011). "Cyber Intelligence. Setting the Landscape for an Emerging Discipline." *Cyber Intelligence Task Force, Intelligence and National Security Alliance*.

35. Franz, George, Galen Kane, and Jeff Fair. (2019). "Reshaping Intelligence Operations in the Cyberspace Domain." *The Cyber Defense Review* 4 (1): 33-40.

36. Gioe, David V. (2017). "'The More Things Change': HUMINT in the Cyber Age." In *The Palgrave Handbook of Security, Risk and Intelligence*, 213-227. Springer.

37. Goldman, Jan. (2015). *The Central Intelligence Agency: An Encyclopedia of Covert Ops, Intelligence Gathering, and Spies [2 Volumes]: An Encyclopedia of Covert Ops, Intelligence Gathering, and Spies*. ABC-CLIO.

38. Gong, Seonghyeon, Jaeik Cho, and Changhoon Lee. (2018). "A Reliability Comparison Method for OSINT Validity Analysis." *IEEE Transactions on Industrial Informatics* 14 (12): 5428-5435.

39. Griffioen, Harm, Tim Booij, and Christian Doerr. (2020). "Quality Evaluation of Cyber Threat Intelligence Feeds." In *International Conference on Applied Cryptography and Network Security*, 277-296. Springer.

40. Guliyev, Fuad. (2010). "National Intelligence Estimate. The Outlook for Intelligence Collection." *Journal of Azerbaijani Studies*.

41. Harrington, Chris. (2013). "Sharing Indicators of Compromise: An Overview of Standards and Formats." *EMC Critical Incident Response Center*.

42. Herman, Michael. (1996). *Intelligence Power in Peace and War*. Cambridge University Press.

43. Higgins, Eliot. (2016). "A New Age of Open Source Investigation: International Examples." In *Open Source Intelligence Investigation*, 189-196. Springer.

44. Hulnick, A. S. (2006). What's wrong with the Intelligence Cycle. Intelligence and national Security, 21(6), 959-979.

45. Hurley, Matthew M. (2012). "For and from Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance." *Air and Space Power Journal* 26 (6): 12-33.

46. Hutchins, Eric M, Michael J Cloppert, and Rohan M Amin. (2011). "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." *Leading Issues in Information Warfare & Security Research* 1 (1): 80.

47. Ilves, Luukas K, Timothy J Evans, Frank J Cilluffo, and Alec A Nadeau. (2016). "European Union and Nato Global Cybersecurity Challenges." *Prism* 6 (2): 126-141.

48. Johnson, David EA, and Newton Howard. (2012). "Network Intelligence: An Emerging Discipline." In *2012 European Intelligence and Security Informatics Conference*, 287-288. IEEE.

49. Johnson, Loch K. (2017). *National Security Intelligence*. John Wiley & Sons.

50. Joint Chiefs of Staff. (2010). *Joint Publication 1-02. Department of Defense Dictionary of Military and Associated Terms*. Department of Defense.

51. Kalkman, Jori Pascal, and Lotte Wieskamp. (2019). "Cyber Intelligence Networks: A Typology." *The International Journal of Intelligence, Security, and Public Affairs* 21 (1): 4–24.

52. Kandiko, Ulises Leon. (2018). "Cyber Intelligence: Reinventing the Wheel." *Triarius. Prevention and Security Bulletin on Terrorism and the New Threats* 2: 27.

53. Kossakowski, Klaus-Peter. (2019). "Computer Security Incident Response Team (CSIRT) Services Framework." FIRST.

54. Kris, David S. (2021). "The NSA's New SIGINT Annex." *Journal of National Security Law & Policy*.

55. Lande, Dmytro, and Ellina Shnurko-Tabakova. (2019). "OSINT as a Part of Cyber Defense System." *Theoretical and Applied Cybersecurity* 1 (1).

56. Leszczyna, Rafał, and Michał R Wróbel. (2019). "Threat Intelligence Platform for the Energy Sector." *Software: Practice and Experience* 49 (8): 1225-1254.

57. Li, Vector Guo, Matthew Dunn, Paul Pearce, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. (2019). "Reading the Tea Leaves: A Comparative

Analysis of Threat Intelligence." In *28th USENIX Security Symposium (USENIX Security 19)*, 851-867.

58. Liew, A. (2007). Understanding data, information, knowledge and their inter-relationships. Journal of knowledge management practice, 8(2), 1-16.

59. Liew, A. (2013). DIKIW: Data, information, knowledge, intelligence, wisdom and their interrelationships. Business Management Dynamics, 2(10), 49.

60. Loleski, Steven. (2019). "From Cold to Cyber Warriors: The Origins and Expansion of NSA's Tailored Access Operations (TAO) to Shadow Brokers." *Intelligence and National Security* 34 (1): 112-128.

61. Lowenthal, Mark M. (2019). *Intelligence: From Secrets to Policy*. CQ press.

62. Lowenthal, Mark M, and Robert M Clark. (2015). *The Five Disciplines of Intelligence Collection*. Sage.

63. Madureira, L., Popovič, A., & Castelli, M. (2021). Competitive intelligence: A unified view and modular definition. Technological Forecasting and Social Change, 173, 121086.

64. McCarthy, Charlie, Kevin Harnett, Art Carter, and Cem Hatipoglu. (2014). "Assessment of the Information Sharing and Analysis Center Model." National Academies Transportation Research Board.

65. McCrory, Duncan. (2020). "Russian Electronic Warfare, Cyber and Information Operations in Ukraine: Implications for NATO and Security in the Baltic States." *The RUSI Journal* 165 (7): 34-44.

66. McMillan, Rob. (2013). "Definition: Threat Intelligence." *Gartner*.

67. Meeuwenberg, Ylona. 2017. "Threat Intelligence Sharing as Part of Supply Chain Management Enhancing Security." PhD thesis, Eindhoven University of Technology.

68. Meier, Roland, Cornelia Scherrer, David Gugelmann, Vincent Lenders, and Laurent Vanbever. (2018). "FeedRank: A Tamper-Resistant Method for the Ranking of Cyber Threat Intelligence Feeds." In *2018 10th International Conference on Cyber Conflict (CyCon)*, 321–344. IEEE.

69. Mocanu, M. (2015). "Intelligence Cycle Model Dilemmas and Solutions." *Romanian Intelligence Studies Review,* (14), 165-178.

70. Mutemwa, Muyowa, Jabu Mtsweni, and Njabulo Mkhonto. (2017). "Developing a Cyber Threat Intelligence Sharing Platform for South African Organisations." In *2017 Conference on Information Communication Technology and Society (ICTAS)*, 1-6. IEEE.

71. North Atlantic Treaty Organization. (2022). "AJP-2.7. Allied joint doctrine for joint intelligence, surveillance and reconnaissance".

72. Noor, Umara, Zahid Anwar, and Zahid Rashid. (2018). "An Association Rule Mining-Based Framework for Profiling Regularities in Tactics

Techniques and Procedures of Cyber Threat Actors." In *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, 1-6. IEEE.

73. Oakley, Jacob G. (2019). "Cyber Collection." In *Waging Cyber War*, 57-70. Springer.

74. Office, NATO Standarization. (2018). *NATO Glossary of Terms and Definitions (English and French)*. NSO.

75. Pawlinski, P, Przemylaw Jaroszewski, Piotr Kijewski, Lukasz Siewierski, Pawel Jacewicz, Przemyslaw Zielony, and Radoslaw Zuber. (2014). "Actionable Information for Security Incident Response." European Union Agency for Network; Information Security.

76. Petratos, Pythagoras. (2011). "Definition and Importance of Cyberintelligence: An Introduction."

77. Phythian, Mark. (2013). *Understanding the Intelligence Cycle*. Routledge.

78. Porche III, Isaac R, Jerry M Sollinger, and Shawn McKay. (2011). "A Cyberworm That Knows No Boundaries." Arlington, VA, USA: RAND Corporation.

79. Price, Douglas R. (2014). "A Guide to Cyber Intelligence." *Journal of US Intelligence Studies* 21 (1): 55-60.

80. Proctor, Tony. (2011). "The Development of Warning, Advice and Reporting Points (WARPs) in UK National Infrastructure." In *International Workshop on Critical Information Infrastructures Security*, 164-174. Springer.

81. Randol, Mark A. (2010). *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*. DIANE Publishing.

82. Richards, Julian. (2014). "The Cyber Challenge for Intelligence." In *Intelligence in the Knowledge Society. Proceedings of the XIXth International Conference*, 97-108.

83. Richelson, Jeffrey T. (2018). *The US Intelligence Community*. Routledge.

84. Richmond, Jeremy. (2011). "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict." *Fordham Int'l LJ* 35: 842.

85. Sari, Arif. (2018). "Context-Aware Intelligent Systems for Fog Computing Environments for Cyber-Threat Intelligence." In *Fog Computing*, 205-225. Springer.

86. Sauerwein, Clemens, Christian Sillaber, Andrea Mussmann, and Ruth Breu. (2017). "Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives." In *Proceedings Der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017)*, 837-851.

87. Saunders, Kimberly. (2000). "Open Source Information: A True Collection Discipline." PhD thesis, Citeseer.

88. Seedyk, Christopher. (2018). "Characterizing Cyber Intelligence as an All-Source Intelligence Product." *DSIAC Journal* 5 (3).

89. Shu, Xiaokui, Frederico Araujo, Douglas L Schales, Marc Ph Stoecklin, Jiyong Jang, Heqing Huang, and Josyula R Rao. (2018). "Threat Intelligence Computing." In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 1883-1898.

90. Shulsky, Abram N, and Gary James Schmitt. (2002). *Silent Warfare: Understanding the World of Intelligence*. Potomac Books, Inc.

91. Staff, Joint Chiefs of. (2013). "Joint Publication 2-0. Joint Intelligence."

92. Steele, Robert David. (2007). "Open Source Intelligence." In *Handbook of Intelligence Studies*, 147-165. Routledge.

93. Strom, Blake E, Joseph A Battaglia, Michael S Kemmerer, William Kupersanin, Douglas P Miller, Craig Wampler, Sean M Whitley, and Ross D Wolf. (2017). "Finding Cyber Threats with ATT&CK™-Based Analytics." MITRE Technical Report MTR170202. The MITRE Corporation.

94. Taneski, Nenad, Aleksandar Petrovski, and Dimitar Bogatinov. (2019). "Geography in Geospatial Intelligence-C4IRS and Cyber Security." In *Security and Crisis Management–Theory and Practice*, 65-73.

95. Taylor, Stan A. (2007). "The Role of Intelligence in National Security." *Contemporary Security Studies*, 249-267.

96. Tekes, R Osman. (2011). "A Common Architecture for Cyber Offences and Assaults-(Organized Advanced Multi-Vector Persistent Attack): Cyber War Cyber Intelligence, Espionage, and Subversion Cyber Crime." PhD thesis, University of London. London, UK.

97. Townsend, Troy, Melissa Ludwick, Jay McAllister, Andrew O Mellinger, and Kate A Sereno. (2013). "SEI Innovation Center Report: Cyber Intelligence Tradecraft Project: Summary of Key Findings." Carnegie–Mellon University. Software Engineering Institute.

98. US Air Force. (2021). "Air Force Doctrine Publication 3-60, Targeting".

99. Williams, Heather J, and Ilana Blum. (2018). "Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise." RAND Corporation.

100. Willis, Brian. (2012). "Sharing Cyber-Threat Information: An Outcomes-Based Approach." Intel Corporation.

101. Xiong, Wenjun, Emeline Legrand, Oscar Åberg, and Robert Lagerström. (2022). "Cyber Security Threat Modeling Based on the MITRE Enterprise ATT&CK Matrix." *Software and Systems Modeling* 21 (1): 157-1.

COMPARATIVE ANALYSIS OF STRATEGIC CYBER SECURITY FOCUS AREAS – UNITED KINGDOM, ESTONIA, ROMANIA

Cristian CONDRUȚ*

Abstract:

Given the fact that cyber-security has a significant impact on many socio-economic sectors and it is dependent on the national context, it is important to analyse the strategic perspective at a national level. Still, by considering that cyber-security strategic topics are being more and more addressed in an international context, it is also relevant to tailor any cyber-security strategy analysis to well-recognized international documents. In this article, we aim to analyse the strategic areas of cyber-security, as they are defined by the International Telecommunication Union, in the manner that those are reflected in the national cyber-security strategies of the United Kingdom, Estonia and Romania. We will highlight some of the common and different elements found in those strategies and will focus more on the Romanian strategy, by making tailored recommendations for each strategic area, based on the International Telecommunication Union Guide.

Keywords: *cyber security, strategy, ITU, UK, Estonia, Romania*.

Introduction

The premise from which we started this research is that cyber-security affects a wide range of sectors of socio-economic development and is influenced by factors dependent on the national context. Thus, the emergence of cyber-security in various sectors of social and economic activity has acquired strategic relevance for states and has led them to adopt national cyber-security strategies. These are the most important

* Teaching assistant, PhD Student in Intelligence and National Security Doctoral School, within National Intelligence Academy "Mihai Viteazul". Email: condrut.cristian@animv.eu

planning document for strategic cyber-security activities and synthesize a particular state's vision of the role it assumes, both for the development of the field at the national level and for the way in which it is related or influences international debates and initiatives (ITU et. al., 2021, p. 34).

The strategic development of the field of cyber-security has been expanded since 2008, when complex state-sponsored cyber-attacks were deployed, with major negative consequences on other states (Shafqat & Masood, 2016, pp. 129-131). Between 2007 and 2010, a series of major cyber-attacks were carried out: the 2007 cyber-attacks in Estonia[1], the 2008 attacks in Georgia and the use of the Stuxnet *worm* in 2010 to disrupt Iran's nuclear infrastructure. These cyber-attacks influenced the adoption of strategic decisions at national and international levels. Most countries with a high level of development in the field of cyber-security adopted their first cyber-security strategy after 2008 (Shafqat & Masood, 2016, p. 131).

An important moment for the development of cyber-security strategies is the year 2018, when *the International Telecommunication Union* (ITU), the specialized organization of the UN, made the first edition of *the Guide to Developing a National Cybersecurity Strategy*. Subsequently, in 2021, the ITU proposed the second edition of the guide, the purpose of which is to provide support for national decision-makers for the development of their cyber-security strategies (ITU et. alii., 2021, p. 8). The ITU approach is of high relevance at the international level, as the ITU guide is the first public document assumed by the UN, which standardizes the good practices of designing and drafting a cyber-security strategy. Section 5 of the ITU Guide is important for our research because it indicates and details how seven strategic focus areas specific to the field of cyber-security should be captured in national cyber-security strategies.

The objective of our research is to carry out a comparative analysis of how the seven strategic focus areas are reflected in three European cyber-security strategies, in order to highlight the common

[1] The time of 22 of days (i.e. between 27 April and 18 May 2007), Infrastructure cybernetics Estonian from Sectors governmental, financial-banking, media online and from the Suppliers of Services Digital at former Target some Attacks cybernetics de tip Distributed Denial of Service.

elements and the differences in the strategic perception of the field of cyber-security in the level of these states. The scope of this research is to assess if any of these countries must undertake any significant efforts in order to better comply with the ITU's Guide recommendations. Thus, this paper could be an instrument for shaping future national cyber-security national strategic policy for any of the three studied nations.

In the next sections, we will present the research methodology, the analysis of the seven strategic focus areas by referring to the strategies and a series of conclusions.

Methodologies

The focus areas of interest in the ITU Guide are: 1) governance; 2) risk management in national cybersecurity; 3) preparedness and resilience; 4) critical infrastructures and essential services; 5) capability and capacity building and awareness raising; 6) legislation and regulation; 7) international cooperation (ITU et. alii., 2021, pp. 34-73). In our approach, these-strategic focus areas will serve as a benchmarking framework for the cyber-security strategies of the states retained for analysis – the United Kingdom, Estonia and Romania. The analysis will be descriptive and explanatory, given that, on the one hand, we will present elements from the national cyber-security strategies, and on the other hand, we will make comparisons between them each related to the strategic focus areas.

We will limit our research to 3 national cyber-security strategies because we are particularly interested in the differences between Romania's strategy and those of the United Kingdom and Estonia, the arguments for choosing each state being:

- *National Cyber Strategy 2022 (NCS UK)* – the choice is based on the fact that the UK is a global cyber power, ranked second globally and first in Europe in the *Global Cybersecurity Index 2020* (ITU Development Sector, 2021, p. 25). The state is at its fourth cyber-security strategy, with the first two being published in 2009 and 2011 (Shafqat & Masood, 2016, p. 131), the third in 2016 (HM Government, 2017) and the fourth in 2022 (HM Government, 2022a), having a rich experience in strategic management of cyber-security.

- *Cybersecurity Strategy 2019-2022* (CS EE) – as mentioned in the introductory section, the choice of Estonia is motivated by the fact that the 2007 cyber-attacks to which it was subjected represent one of the critical points of the field of cyber-security. Those cyber-attacks fundamentally changed the traction that the domain has begun to receive at the strategic level. Moreover, the Estonian Ministry of Economic Affairs and Communications (MAEC Estonia) mentions at the beginning of the document the events of 2007, classifying them as the only ones that have affected the Estonian informational society (MAEC Estonia, 2019, p. 11). For this reason, Estonia represents a European model in terms of digital transformation of public services, ranking first in this category in the *Digital Economy and Society Index*[2] (European Commission, 2022), which justifies the inclusion of the strategy in the present research.
- *Romania's cybersecurity strategy for the period 2022-2027* (SSCR RO) – the main argument is that our most important interest is in the situation of the strategic perception of cyber-security at the national level of Romania and how it can be compared to those presented in the strategies of the United Kingdom and Estonia. The secondary argument is that the present research will be part of a broader doctoral research that will be carried out in relation to the national cyber-security context and will address the topic of cyber-security education.

Analysis of strategic focus areas of cyber-security

In *Table 0* we present the strategic focus areas of cyber-security and the specific areas of each. We will comparatively analyse the strategic focus areas of cyber-security and will lay out in *Tables 1 – 7*, our assessment of the way that ITU recommendations are implemented for each specific area in the case of NCS UK, CS EE and SSCR RO.

[2] Index Measured the Level States member EU that Measured Level of Digitization, through reporting the Parameters as capital human, integrate a Technologies Digital and Services Public Digital.

Table 0[3]: Correspondence between strategic focus areas and specific areas recommended to be captured in a national cyber-security strategy. Data retrieved *from the Guide to Developing a National Cybersecurity Strategy* (ITU et. alii., 2021).

Strategic focus areas	Specific areas
1. Governance	• Ensure the highest level of support; • Establish a competent cybersecurity authority; • Ensure intra-governmental cooperation; • Ensure inter-sectorial cooperation; • Allocate dedicated budget and resources; • Develop an implementation plan.
2. Risk management in national cybersecurity	• Conduct cyber threat assessment to align policies with the ever-expanding cyber threat landscape; • Define a risk-management approach; • Identify a common methodology for managing cybersecurity risk; • Develop sectorial cybersecurity risk profiles; • Establish cybersecurity policies.
3. Preparedness and resilience	• Establish cyber-incident response capabilities; • Establish contingency plans for cybersecurity crisis management and disaster recovery; • Promote information-sharing; • Conduct cybersecurity exercises; • Establish impact and severity assessment of cybersecurity incidents.
4. Critical infrastructures and essential services	• Establish a risk-management approach to identifying and protecting critical infrastructures and essential services; • Adopt a governance model with clear responsibilities; • Define minimum cybersecurity baselines; • Utilise a wide range of market levers; • Establish public-private partnerships.
5. Capability and capacity building and awareness raising	• Strategically plan capability and capacity building and awareness raising; • Develop cybersecurity curricula; • Stimulate capacity development and workforce training;

[3] The table was also presented within the Doctoral Research Project, elaborated as a part of the doctoral research program of the author.

	• Implement a coordinated cybersecurity awareness-raising programme; • Foster cybersecurity innovation and R&D • Tailored programmes for vulnerable sectors and groups.
6. Legislation and regulation	• Establish a domestic legal framework for cybersecurity; • Establish a domestic legal framework for cybercrime and electronic evidence; • Recognise and safeguard human rights and liberties; • Create compliance mechanisms • Promote capacity-building for law enforcement; • Establish inter-organizational processes; • Support international cooperation to combat cyber threats and cybercrime.
7. International cooperation	• Recognise cybersecurity as a component of foreign policy and align domestic and international efforts; • Engage in international discussions and commit to implementation. • Promote formal and informal cooperation in cyberspace; • Promote capacity building for international cooperation.

Governance. The designation of a competent authority and the assurance of inter-sectorial cooperation are the only elements satisfied in all strategies. The unitary nature of this common dimension is explained by the existence of Directive 2016/1148 of the European Parliament and of the Council on improving the level of cyber-security of network and information systems at the EU level (i.e. the NIS Directive), the EU Member States being obliged to designate such an authority (European Union, 2016, p. 6). With regard to cross-sectorial cooperation, all strategies refer to the public-private partnership. One of the most significant differences is captured in the dimension of ensuring the highest level of support, given that SSCR RO is not assumed by a high representative of the state, as it happens in the case of NSC UK. In order to be in line with the ITU Guide, Romania should include in the future cyber-security strategy the declaration of support of a high representative of the state, present more extensively the mechanisms of

intra-governmental cooperation and allocate estimated resources for the field of cyber-security.

Table 1: Summary representation of the strategic *governance area*. Source: author

Governance	Highest level of support	Competent authority	Intra-governmental cooperation	Inter-sectorial cooperation	Budget and resource allocation	Implementation plan
NCS UK	Present	Present	Present	Present	Present	Present
CS EE	Unidentified	Present	Present	Present	Partially	Partially
SSCR RO	Unidentified	Present	Partially	Present	Partially	Present

NCS UK – The document defines how public institutions at the UK level will apply the strategy's provisions. On the one hand is being mentioned the control body over the implementation of the strategy's action plan – *The National Security Council* – and on the other hand, the public entities that have clear roles and responsibilities for implementation (HM Government, 2022a, p. 112). The most important governmental actor involved is the *National Cyber Security Centre*, defined as the technical authority for cyber threats (HM Government, 2022a, p. 128). For *intra* and *inter*-governmental cooperation, the document promotes *the whole-of-society* vision, which involves defining roles and responsibilities throughout British society and capitalizing on partnerships between relevant actors (HM Government, 2022a, p. 50). Regarding the financial resources allocated to the domain, the document provides for the sum of 2.6 billion pounds for the development of the IT and cyber-security sectors (HM Government, 2022a, p. 115). Although the UK strategy does not include a separate action plan, the implementation section presents the related strategic targets and objectives with deadlines for implementation (HM Government, 2022a, pp. 46 – 97).

CS EE – The document clearly defines the responsibilities of each Estonian government institution, as well as the links between the national cyber-security strategy and other government strategies (e.g., Estonia's Digital Agenda 2020, Lifelong Learning Strategy 2014-2020) (MAEC Estonia, 2019, pp. 29-32). The competent authority for the implementation of the provisions of the cyber-security strategy is MAEC Estonia and the strategic coordination is ensured by the Cyber Security Council of the Governmental Security Council (MAEC Estonia, 2019, p. 33). For intra-governmental cooperation, MAEC Estonia organizes these actions at the national level, including the exchange of information between responsible officials (MAEC Estonia, 2019, p. 36). Beyond the role of guiding and structuring the strategic steps associated with the field of cyber-security, the Estonian strategy was also created as a means of communication to improve public-private partnerships (MAEC Estonia, 2019, p. 8), support and promote cyber-security research and development (R&D) (MAEC Estonia, 2019, p. 52) and develop public and private sector talent. The strategy does not provide for the allocation of a fixed amount of budget but plans to adopt one based on the activities carried out in 2020 (MAEC Estonia, 2019, p. 32). It also does not provide for a specific implementation plan, with the responsibility being delegated to competent authorities (MAEC Estonia, 2019, p. 32).

SSCR RO – Although the strategy is adopted with a decision of the Romanian Government, it is not assumed by a high governmental representative. At the strategic level, the coordination of cyber security approaches in Romania is ensured by the Cyber Security Operational Council (COSC), subordinated to the Supreme Council of National Defence (Romanian Government, 2022, p. 19). The effective implementation of the actions provided for in the strategy is achieved through the involvement of several governmental institutions, the central role in this regard is ensured by the National Directorate of Cyber Security (DNSC) (Romanian Government, 2022, p. 20). Although the development of intra-governmental cooperation is one of the responsibilities of the DNSC, the COSC is the "inter-institutional cooperation mechanism" (Romanian Government, 2022, p. 19). The inter-sectorial cooperation component is addressed by establishing measures aimed at strengthening the public-private partnership

(Romanian Government, 2022, pp. 21-23). The Romanian Government encourages the allocation of budget and resources to a wide range of actors in society, without providing clear information in this regard (e.g., an estimated budget or certain fiscal policies). The strategy also contains an implementation plan, in which the strategic objectives are correlated with the measures and actions necessary to be implemented while establishing the participant and responsible entities and the deadlines for the implementation (Romanian Government, 2022, pp. 30-48).

Risk management in national cybersecurity

Establishing cyber-security policies is the only specific area that is fulfilled in all 3 strategies and we argue that it is correlated to the NIS Directive, transposed into the national legislation of all 3 states. It provides for the implementation of minimum cybersecurity baselines for operators of essential services and digital service providers. The comparative analysis of the 3 strategies shows that the risk management situation is different at the level of each state, given that the UK has fulfilled most of the recommendations in the ITU Guide: 4 out of 5; Estonia – 3 out of 5; Romania – 1 out of 5. For a future cyber-security strategy of Romania, it is necessary to present and promote approaches and methodologies of risk management, as well as to establish cyber-security risk profiles for citizens, and public and private entities.

Table 2: Summary representation of the *risk management in national cyber-security area*.
(Source: author's view)

Risk management	Cyber threat assess-ment	Risk manage-ment approach	Methodology for risk management	Risk profiles	Cyber-security policies
NCS UK	Partially	Present	Present	Present	Present
CS EE	Present	Partially	Present	Uniden-tified	Present
SSCR RO	Partially	Uniden-tified	Unidentified	Uniden-tified	Present

NCS UK – The document presents a brief strategic assessment of the cyber threat, based on the premise that cyber-space is an environment created and influenced by human behaviour (HM Government, 2022a, p. 17). Thus, one of the objectives assumed by the UK Government is to improve the understanding of cyber risks in order to carry out actions to strengthen cyber-security and resilience (HM Government, 2022a, p. 68). The strategy presents previous efforts to understand cybersecurity threats, including large-scale adoption of a conceptual framework (CAF – Cyber Assessment Framework) for assessing existing risks at the level of critical cyber infrastructures (HM Government, 2022a, p. 68). The UK has transposed into national legislation the NIS Directive, which defines technical and organizational measures for sectors providing essential services to the population (i.e., energy, transport, health and drinking water) and sectors that make digital services available (i.e., *cloud computing* services, search engines, online marketplaces). The document presents cyber-security policies, an example being the optimization of the government's vulnerability reporting programme – *Vulnerability Reporting Service*.

CS EE – Estonia's strategy begins by conducting a cyber-security national assessment, structured on three subchapters: 1) trends affecting the state of cyber-security (e.g., emerging technologies, development of cybercrime-as-a-service phenomenon, complicated geopolitical and security situation); 2) Estonia's strengths (e.g., efficiency and flexibility of a small state, Estonia's international influence) and 3) challenges to cyber-security of Estonia (e.g. lack of integrated *leadership*, insufficient understanding of the interdependencies between cyber threats; lack of specialists and training of new specialists) (MAEC Estonia, 2019, pp. 19-28). The methodological framework of risk management is provided by the *Law on Crisis Management*[4] and the *Law on Cyber-Security*[5], the need for improvement on this component is

[4] Estonian Law on Crisis Management available in English at https://www.riigiteataja.ee/en/eli/525062014011/consolide, accessed on 07.02.2023.

[5] Estonian Law on Cyber-Security is the national law transposing the EU Directive 2016/1148 on measures for a high common level of security of network and information systems in the Union (NIS Directive) and EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the

generated by the implementation in practice of the two normative acts (MAEC Estonia, 2019, p. 45). For cyber-security policies, MAEC Estonia mentions a number of programs, such as the ITC sector development one or *Targalt Internetis.*[6]

SSCR RO – It is presented a cyber-threat assessment structured according to the activities carried out by state actors, cyber-crime groups and ideologically or politically motivated hacker groups (Romanian Government, 2022, p. 7). However, the assessment is not carried out by highlighting risks to critical infrastructures as recommended in the ITU Guide, nor does it identify these infrastructures (ITU et. alii., 2021, p. 37). The Romanian Government does not present a risk management approach but includes in the action plan measures aimed at developing and implementing future methodologies for assessing the level of cyber-security (Romanian Government, 2022, pp. 30-31). The Romanian Government encourages the creation and implementation of a minimum set of cyber-security policies and disaster recovery plans (Romanian Government, 2022, p. 16).

Preparedness and resilience

Promoting information exchange and conducting cyber-security exercises are the only areas common to the 3 analysed strategies. The promotion of information exchange is a natural consequence of public-private partnership and the involvement of different types of actors in strengthening national cyber resilience. The cyber security exercises are carried out through the direct involvement of all 3 states, which have either the role of organizer or participant. The only area not addressed within SSCR RO is assessing the impact and severity of cyber-security incidents, being necessary to encourage this practice in the future cyber-security strategy, by reference to how critical goods, services, infrastructure and citizens are affected (ITU et. alii., 2021, p. 41).

---

free movement of such data (GDPR Regulation). Available in English at https://www.riigiteataja.ee/en/eli/523052018003/consolide, accessed on 07.02.2023.

[6] The project whose mission is to develop the skills of children and parents for the use of the Internet. The information is available on https://www.targaltinternetis.ee/en/about-the-project/ and was accessed on 07.02.2023.

Table 3: Summary representation of the *preparedness and resilience area*. (Source: author's view)

Preparedness and resilience	Cyber-security incident response capabilities	Contingency plans and crisis management	Promote sharing of information	Cyber-security exercises	Assessment of the impact and severity of cyber-security incidents
NCS UK	Present	Present	Present	Present	Present
CS EE	Partially	Partially	Present	Present	Partially
SSCR RO	Present	Partially	Present	Present	Unidentified

NCS UK – The UK strategy addresses the cyber resilience component in an exhaustive manner, given that one of the major strategic dimensions is of developing a digital, prosperous and resilient UK. UK's vision is segregated into three major areas: understanding the risks; acting to secure information systems and networks; developing cyber resilience to minimise the impact of cyber incidents and improve recovery capacity (HM Government , 2022a, p. 65). The UK Government defines objectives and proposes measures to strengthen cyber resilience through cyber-security incident response capabilities – both through teams and technical authorities, as well as through law enforcement organisations – by adopting contingency plans (i.e., *cyber incident response schemes*), by exchanging *intra* and *cross*-sectorial information, by conducting cyber-security exercises (i.e. *Cyber Incident Exercising service*) (HM Government, 2022a, pp. 64 – 77) and by assessing the impact and severity of cyber-security incidents (HM Government, 2022a, p. 125).

CS EE – The Estonian strategy makes only one reference to the existence of an institution that has responsibilities for responding to cyber-security incidents – *the Computer Emergency Response Team* (CERT). Although within the ITU Guide (ITU et. alii., 2021, p. 39) it is recommended that such an institution also has responsibilities in terms of vulnerability management, situational awareness or educational services, CERT-EE has responsibilities only in terms of cyber security

incident management (Information System Authority, n.d.). The strategy states that crisis management activities, integration of cyber-security with defence planning and crisis management preparedness are carried out through joint cybersecurity exercises (MAEC Estonia, 2019, p. 47). The promotion of information exchange is seen in direct connection with the mitigation of cyber-security risks (MAEC Estonia, 2019, p. 46), with the bilateral cooperation dimension being accentuated through activities aimed at carrying out joint analyses, exchanges of good practices and technical information (MAEC Estonia, 2019, p. 59). One of Estonia's main strategic directions is cyber-security exercises, given the rich history of hosting and involvement in such activities, an important example in the context being *the NATO Locked Shields* exercise, organized CCDCOE (CCDCOE, n.d.). There is no particular reference to cyber-security assessments based on the impact on essential goods, services, infrastructures and citizens, as recommended by the ITU Guide (ITU et. alii., 2021, p. 41). However, the Estonian Police and the Estonian Internal Security Service (i.e., KAPO) are responsible for carrying out integrated assessments of the state of cyber-security at the national level (MAEC Estonia, 2019, p. 35).

SSCR RO – Within the strategy is mentioned the measure of creating CERTs and Security Operational Centres (SOCs) by sectors of activity (Romanian Government, 2022, pp. 23-24), as a part of the objective of developing cyber resilience at a national level, thus being satisfied the recommendation from the ITU Guide on encouraging the development of capabilities for responding to cyber-security incidents (ITU et. alii., 2021, p. 39). With regards to the adoption of contingency plans, this practice is encouraged in the strategy, without any reference to the crisis management component (Romanian Government, 2022, p. 16). Furthermore, the action plan requires the exchange of information between certain public institutions and private entities on a permanent basis (Romanian Government, 2022, p. 32). Cyber-security exercises are presented as a good opportunity to test resilience and response capabilities and cooperation mechanisms (Romanian Government, 2022, p. 24).

Critical infrastructures and essential services

None of the specific areas of this strategic focus area is fulfilled in all three strategies, however there are three areas for which NCS UK and

CS EE meet the recommendations of the ITU. Romania's approach on this dimension is too general, given that the SSCR RO does not refer to any risk management approach or any governance model and it is not detailed how the state will capitalize on public-private partnerships. Although there are references to all these areas by correlation with other strategic focus areas (e.g., governance, risk management), none of them is customized in the context of operators of essential services or digital service providers. It is necessary for Romania's future cyber-security strategy to pay more attention to this dimension, considering, on the one hand, the regional security context – the use of cyber tools in the Russian-Ukrainian War – and on the other hand the adoption at EU level of the NIS 2 Directive[7] at the end of 2022.

Table 4: Summary representation of the *critical infrastructures and key services area*. (Source: author's view)

Critical infra-structures and essential services	Risk management approach	Governance model	Minimum cyber-security baselines	Wide range of market levers	Public-private partnerships
NCS UK	Present	Present	Present	Present	Present
CS EE	Present	Unidentified	Present	Present	Partially
SSCR RO	Unidentified	Unidentified	Partially	Partially	Unidentified

NCS UK – Government's UK institutions must lead by example other national entities in understanding cyber-security risks. The UK government aims to adopt CAF on a large scale, to gain a better understanding of how critical infrastructures depend on supply *chains*, to improve partnerships with managers and operators of critical infrastructure, and to obtain a better understanding of the risks posed by

[7] It is the update of the NIS Directive and directly introduces the rule on the threshold by size, without leaving this to the discretion of the Member States. Information available at https://www.consilium.europa.eu/ro/press/press-releases/2022/11/28/ eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/ on 23.02.2023.

accelerated digitalisation (HM Government, 2022a, p. 68). The UK's governance model appoints the authorities responsible for coordinating the implementation of cyber-security measures for critical infrastructures at national level (HM Government, 2022a, p. 124). The UK's Government encourages the fulfilment of the minimum cybersecurity baselines set by the competent authorities for operators of essential services defined in the national legislation transposing the NIS Directive (HM Government, 2022a, p. 71). The public-private partnership is reflected in the UK's strategy by adopting special laws to create facilities for organisations that pose a high cyber-security risk. In addition, cooperation and dialogue with influential economic actors (e.g., investors, financial institutions or auditors) will encourage the large-scale adoption of cybersecurity best practices for the UK's economy (HM Government, 2022a, p. 72).

CS EE – The risk management approach in Estonia is presented as being in relation to the implementation in practice of the Cybersecurity Law and the Crisis Management Law. Since the Cybersecurity Act transposes the NIS Directive into the national regulatory framework and because it also refers to operators of essential services, it can be concluded that Estonia presents in the strategy a risk management approach for critical infrastructures and essential services. Estonia's minimum cybersecurity baselines are based on one of Germany's policies in the field: *the BSI IT-Grundschutz* (MAEC Estonia, 2019, p. 42), which is the minimum standard of cyber-security measures for computer systems and networks (Information System Authority, 2022). However, ISKE (i.e., the Estonian adaptation of the German standard) has raised many issues for public authorities in Estonia, strategy proposing systematization of criteria and the centralized provision of cyber-security services for implementation at the level of government institutions, private companies, NGOs and citizens (MAEC Estonia, 2019, p. 42). Given the wide range of entities covered by minimum cybersecurity standards, the strategy also refers to the policy-making component to encourage organisations and individuals to strengthen their cyber-security. While no direct reference is made to the development of the public-private partnership to ensure the cyber-security of critical infrastructures and essential services, the very establishment of minimum cybersecurity

standards across Estonian society can facilitate development on this component.

SSCR RO – Romania's strategy encourages the practice of adopting a minimum set of cyber security baselines at the level of each entity that operates information systems or networks (Romanian Government, 2022, p. 16). However, no reference is made to the adoption of such measures for operators of essential services or digital service providers. The Romanian Government encourages the creation of a unified regulatory framework in the field of cyber-security measures and policies and the provision of training formats for cyber-security experts (Romanian Government, 2022, p. 16), without customizing on the context of operators of essential services and digital service providers.

Capability and capacity building and awareness raising

The only two areas that comply with the recommendations of the ITU Guide in all 3 strategies are strategic planning and the implementation of a coordinated programme to raise awareness. Roles and responsibilities for the implementation of measures aimed at developing capabilities, capacities and awareness are clearly defined in all three strategies. Coordinated *awareness* programmes at the population level are supported by concrete elements or projects in all three strategies. However, the creation of curricular frameworks, the development of training formats for the workforce or the development of research, innovation and development are areas that require increased attention for future cyber-security strategies, especially from Romanian side. We found that SSCR RO generally encourages the development of measures for these areas, but without promoting existing or planned projects to be carried out, compared to NCS UK and CS EE, which present concrete initiatives.

Table 5: Summary representation of the *capability and capacity building and awareness raising area*. (Source: author's view)

Capability and capacity building and awareness raising	Strategic planning	Curricular frameworks	Workforce training	Coordinated awareness programme	Research, innovation and development in cyber-security	Tailored programmes for vulnerable groups and sectors
NCS UK	Present	Partially	Present	Present	Present	Unidentified
CS EE	Present	Present	Partially	Present	Present	Partially
SSCR RO	Present	Partially	Partially	Present	Partially	Unidentified

NCS UK – UK runs a number of projects, predominantly managed by *the National Cyber Security Centre* (NCSC) or the *National Crime Agency* (NCA), such as *NCA Cyber Choices* and *NCSC Cyber Aware*, although there is no authority specifically designated in the strategy to implement the capability, capacity and awareness development programmes. Cyber-security education is predominantly treated in relation to the specialization and diversification of the workforce in the field, the UK Government's approach being *a whole-of-society* one, which implies the involvement of all actors from the British society in the training of future specialists in cyber-security and in which public institutions, private companies and the academic environment subsequently benefit from their training. In addition, the UK Government is paying close attention to academia, stating that at national level are 19 centres of academic excellence in cyber-security, whose curricula will be aligned with cyber-security industry standards by 2030 (HM Government, 2022a, p. 52). In the UK there are 19 centres of academic excellence and 4 research institutes on cyber-security issues (HM Government, 2022a, p. 21). The UK Government's vision of RDI is captured within the strategic objective of improving the ability to anticipate, evaluate and act on advances in science and technology, vital to maintaining the UK's *status quo* of cyber power (HM Government, 2022a, p. 81). The UK Government aims to better analyse technological and scientific advances in cyber-security to better understand the

strategic implications they entail (HM Government, 2022a, p. 81). In order to improve and sustain its own and allied technological advantage, the UK Government encourages academia to better cooperate with the private cyber-security industry to promote and operationalise research results (HM Government, 2022a, p. 83). Another objective of the UK Government is to encourage communities made up of actors from multiple sectors of society to develop technological standards in priority areas that safeguards democracy principles and improve the level of cyber-security (HM Government, 2022a, p. 88).

CS EE – Strategic planning of capability development and awareness raising is well articulated in the Estonian strategy. *State Information System Authority* (RIA) has responsibilities to develop technological resilience, to raise awareness of general population and to coordinate research and development in cyber-security and the Ministry of Education and Research deals with the harmonisation of the objectives of this strategy with the Lifelong Learning Strategy 2014-2020. Relating to curricular frameworks, Estonia deals exhaustively with the subject in relation with different educational stages. However, at least three aspects are assumed by MACE Estonia as problematic in terms of curricular frameworks in the field of cyber-security: 1) lack of conceptual links between private sector needs and the cyber-security competence framework (MAEC Estonia, 2019, p. 70); 2) lack of unitary practices in the continuous professional training of specialists in the public sector (MAEC Estonia, 2019, p. 89); 3) limited existence of tools to measure cyber-security knowledge and skills (MAEC Estonia, 2019, pp. 67-68). For awareness programmes in the field of cyber-security, MACE Estonia aims to carry out projects adapted for different social groups: the general public, students and teachers, government institutions and local public institutions and high-level officials of the Estonian state (MAEC Estonia, 2019, pp. 66-69). One of the major strategic objectives is the industry development and cyber-security research. The achievement of this objective depends on capitalising on cooperation between organisations in the public, private and academic sectors, on the realisation of a national R&D plan in the field of cyber-security, on the provision of state support for innovation and on ensuring a beneficial environment for the development of *start-ups* (MAEC Estonia, 2019, pp. 52-54). The only

vulnerable group to cyberattacks, which often lacks the capacity to ensure an adequate level of cyber-security are the small companies, RIA Estonia Providing support in the event of the materialization of cyber-security incidents (MAEC Estonia, 2019, p. 66).

SSCR RO – Strategic planning is ensured by adopting the action plan of the cyber-security strategy. Although the Romanian Government encourages the development of cyber-security educational programmes in all educational stage – "since the primary school" (Romanian Government, 2022, pp. 21-22) – it does not propose the adoption of curricular frameworks for cyber-security. In terms of training formats for the labour market, the strategy encourages the strengthening of the level of technical knowledge and the development of behaviours for mitigating cyber-security risks (Romanian Government, 2022, p. 22). However, the recommendations made in the ITU Guide are being followed to a small extent, as the definition of career trajectories or schemes for the training of cyber-security specialists are not encouraged (ITU et. alii., 2021, p. 45). With regards to cyber threat awareness, multiple activities are state in the action plan (Romanian Government, 2022, pp. 38-39). The strategy provides for a series of measures for the development of the field of cyber-security research and innovation, the Romanian Government supporting the cooperation with the private and academic environment, the involvement of the research community in European networks in the field or the additional allocation of governmental financial resources. However, the strategy does not encourage access to research grants or the development of research programmes and the dissemination of research results, as recommended in the ITU Guide (ITU et. alii., 2021, p. 46).

Legislation and regulation

The creation of compliance mechanisms is the only area for which the recommendations of the ITU Guide are followed in all 3 strategies, given that the NIS Directive has been transposed into the national legislation of all 3 states. However, all 3 states have gaps in the establishment of a national legal framework for cyber-security, since none of the 3 strategies refer to a law in force regulating institutional roles and responsibilities in the field. The field of cybercrime is not

presented in the SSCR RO in terms of legislative, cooperation or capability building, unlike NCS UK or CS EE, which encourages the amendment of criminal legislation, defines institutional responsibilities and presents concrete cases of international cooperation to combat cybercrime. With regards to Romania's strategy, cybercrime field is not being sufficiently addressed, being necessary to approach and detail this dimension in the future cyber-security strategy of Romania.

Table 6: Summary representation of the *legislation and regulation area*. (Source: author's view)

Legislation and regulation	Domestic legal framework	Domestic legal framework in the field of cybercrime and digital evidence	Recognition and protection of human rights and liberties	Creation of compliance mechanisms	Capacity building for law enforcement	Establishment of inter-organizational processes	Supporting international cooperation to fight cyber threats and cybercrime
NCS UK	Partially	Partially	Present	Present	Present	Present	Present
CS EE	Partially	Partially	Partially	Present	Present	Present	Partially
SSCR RO	Partially	Unidentified	Partially	Present	Unidentified	Partially	Unidentified

NCS UK – The legal framework in the field of cyber-security is composed of the national law transposing the NIS Directive and the one transposing the European GDPR Regulation (HM Government , 2022a, p. 65). With regards to the legal framework in the field of cybercrime and electronic evidence, it is stipulated that the *Counter State Threats Bill* – which is part of the UK's national security package (HM Government, 2022b) – must be amended to cover national security threats from cyberspace. In order to optimise the roles and responsibilities of law enforcement institutions for cyber-security offences, the UK's Government is promoting the need to amend the *Proceeds of Crime Act 2002* (HM Government, 2022a, p. 104). The UK's government recognises the importance of fundamental human rights and freedoms in the context of countering digital authoritarian movements and abusive state

control (HM Government, 2022a, p. 34). Enforcement of compliance mechanisms is ensured by the competent authorities for the coordination and application of the legislation transposing the NIS Directive (HM Government, 2022a, p. 122). The promotion of the development of law enforcement capabilities is captured in one of the most consistent chapters of the strategy, which is about countering threats. New investments are foreseen here to provide law enforcement agencies with the capabilities they need to conduct investigations and maintain their technological advancement compared to adversaries (HM Government, 2022a, p. 100). Given that the UK's strategy is created by adopting the *whole-of-society* vision, the component of inter-organisational processes is approached in relation to this principle. Beyond the wide range of already existing public enforcement institutions, such as the NCSC, NCA, Government Communications Headquarters (GCHQ) or Ministry of Defence (MoD), in 2020 the National Cyber Force (NCF) was created whose responsibility is to operate *in* and *through* cyberspace to counter, disrupt, degrade and challenge entities with hostile intentions against the UK. The NCF conducts operations to influence individuals or groups, to disrupt online communication systems or to degrade physical systems, all of which are defined in the strategy as *cyber offensive* (HM Government, 2022a, pp. 41-42). The importance of the international cooperation dimension in countering cyber threats and cybercrime is recognised and encouraged in the UK strategy and integrated into British government's endeavours (HM Government, 2022a, p. 104).

CS EE – The main elements of cyber-security regulatory framework in Estonia are the Cybersecurity Law and the Crisis Management Law. The legislative framework on cybercrime is represented by the Estonian Criminal Code, which defines the offences such as obtaining illegal access to information systems (Estonian Parliament, 2015). One of the four principles on which the Estonian strategy is based refers to the equal importance of protecting and promoting fundamental rights and freedoms, both in physical and cyberspace. However, during the course of the strategy, the subject is not elaborated. The subject of compliance mechanisms is extensively addressed within the strategic objective aimed at affirming Estonia as a

sustainable digital state, the standard of minimum cybersecurity baselines, ISKE (a topic also addressed in the critical *infrastructures and essential services* section) being adopted (MAEC Estonia, 2019, p. 42). The development of the capabilities and capacities of the law enforcement institutions is carried out through the Internal Security Development Plan 2021 – 2030, which includes activities such as promoting the capabilities of detection and investigation of cybercrime activities, promoting cooperation at national and international level or analysing and reducing the risks to *the e-Residency*[8] systems and digital identity[9] (MAEC Estonia, 2019, p. 30). The organizational processes related to the fight against cybercrime are detailed in the strategy, the main institutions responsible for this component being the Ministry of Justice, the Office of the Prosecutor General's, the Data Protection Inspectorate, the Estonian Forensic Science Institute or the Centre of Registers and Information Systems (MAEC Estonia, 2019, p. 34). With regards to international cooperation in the field of cybercrime, certain elements (e.g., cooperation formats, international treaties in the field) are not particularly articulated, but it is proposed to create a framework for cooperation and information exchange through which capabilities will be strengthened.

SSCR RO – Given the fact that SSCR RO was adopted in December 2021, it is not mentioned the fact that Romania has recently adopted a national law concerning cyber-security and cyber-defence – Law 58/2023[10]. This law regulates responsibilities regarding information networks and systems that are used, organised, administered or possessed by public and private entities, including citizens. It also regulates the strategic and operational cyber-security framework in

[8] Digital system through which any person can obtain a digital business identity registered in the records of the Estonian state, online and in about 15 minutes. Information available at https://www.e-resident.gov.ee/, on 10.02.2023.

[9] Digital system through which any Estonian citizen can obtain a digital personal identity that he can use for digital signing, online voting or access to personal medical and tax data. Information available at https://e-estonia.com/solutions/e-identity/id-card/, on 10.02.2023.

[10] Law concerning cyber-security and cyber-defence was adopted on March 14, 2023 and is available in Romanian language at https://monitoruloficial.ro/Monitorul-Oficial--PI--214--2023.html. It was accessed on March 16, 2023.

Romania, regarding cyber-incident response, cyber resilience, national and international cooperation, research and development, cyber-education, crisis management, but also enforces penalties for entities that do not comply with the law (Romanian Parliament, 2023). Another important legislative element is 2018 the Law 362/2018 on ensuring a high common level of security of network and information systems, which transposes the provisions of the NIS Directive, was adopted (DNSC, n.d.). Within the Romanian strategy there are no references to elements of normative framework in the field of cybercrime, although Romania is a signatory state of the Budapest Convention (Council of Europe, n.d.) and that the Law 286/2009 (i.e., the Criminal Code) provides for a series of "crimes against the safety and integrity of information systems" (Romanian Parliament, 2009). Although the adoption of a cyber-security regulatory framework that falls within the limits of the international legislation on human rights and fundamental freedoms is encouraged, the existing recommendation in the ITU Guide on accentuating contextual differences between cyber-security (i.e., understood in a technical way) and cybercrime (i.e., understood as a process of applying criminal legislation) (ITU et. alii., 2021, p. 48) is not respected. The creation of compliance mechanisms is encouraged for all network operators and information systems, and in particular for entities designated under the legislation transposing the NIS Directive (Romanian Government, 2022, p. 16). With regards to the inter-organisational processes, multiple actors are designated in the implementation plan of the strategy to participate in the implementation of the measures assumed in the document. However, some elements recommended in the ITU Guide, such as judicial cooperation and compliance with national and international legislation in the field of cybercrime (ITU et. alii., 2021, pp. 49-50), are not defined or addressed in the Romanian strategy.

International cooperation

International cooperation is a well-represented strategic area in all of the 3 strategies. Each of the three states recognizes that cyber-security is an integral part of foreign policy and promotes the need to engage in international discussions. In Romania’s case, it is necessary to

present punctual initiatives and projects to promote formal and informal cooperation, but also to develop the capacity for international cooperation.

Table 7: Summary representation of the *international cooperation* strategic *area*. (Source: author's view)

International cooperation	Recognizing cyber-security as a component of foreign policy	Engagement in international discussions and commitment to implementation	Promoting formal and informal cooperation in cyberspace	Promoting capacity building for international cooperation
NCS UK	Present	Present	Present	Present
CS EE	Present	Present	Present	Present
SSCR RO	Present	Present	Partially	Partially

NCS UK – Cyber-security is perceived by the UK's Government as a central component of the foreign policy conducted by the state, given that each of the proposed strategic objectives requires international involvement (HM Government, 2022a, p. 36). Involvement in international discussions on cyber-security issues is based on the UK's cybersecurity status, one of the strategic objectives being to influence global governance to promote a safe, open and free cyber-space (HM Government, 2022a, p. 94). The UK is involved in cooperation formats (e.g., *Five Eyes*, G7) or is an important part of organisations such as the UN, the EU or the World Bank (HM Government, 2022a, p. 93). The UK's involvement in international cooperation activities is illustrated both by activities aimed at strengthening cyber capabilities for states in Eastern Europe, Africa and the Indo-Pacific (HM Government, 2022a, p. 92), as well as by the use of all available cooperation channels – foreign policy or law enforcement organisations (HM Government, 2022a, p. 93). The UK Government promotes the development of the capacity for international cooperation by recognising the importance of diplomatic measures on cyber-security and by harnessing the external influence of the state (HM Government, 2022a, p. 91).

CS EE - One of the most articulated components of the Estonian strategy is the recognition of cyber-security as an integrated part of the state's foreign policy. There are many initiatives carried out by the Estonian authorities, such as the inclusion of the cyber-security field in the Foreign Policy Development Plan 2030 and in the Development Plan for Cooperation and Humanitarian Aid 2016-2020 (MAEC Estonia, 2019, p. 31); hosting the NATO CCDCOE in Tallinn (MAEC Estonia, 2019, p. 72); Estonia's participation in regional and international cooperation formats, within organizations such as NATO, the EU or the OSCE (MAEC Estonia, 2019, pp. 58-61). Estonia encourages formal and informal cooperation in the field of cyber-security as a measure to achieve all the objectives proposed in the strategy, addressing dimensions such as public-private partnership, cooperation by law enforcement institutions or cooperation with strategic partners from other states or international organisations. Given that the dimension of international cooperation is found in all the strategic objectives assumed by the Estonian State, measures to develop the capacity for international cooperation, such as the inclusion of cyber-security experts in organisations with responsibilities outside Estonian territory, are also promoted in the strategy (MAEC Estonia, 2019, p. 59).

SSCR RO - Although it is not mentioned in the Romanian strategy that cyber-security must represent a part of the state's foreign policy, as recommended in the ITU Guide (ITU et. alii., 2021, p. 51), the Romanian Government assumes that the country will become a relevant actor in the international cooperation architecture (Romanian Government, 2022, p. 24). According to the Romanian Government, this objective can be achieved by strengthening Romania's role at global and regional level, in bilateral relations and by strengthening *cyber-diplomacy* (Romanian Government, 2022, pp. 23-27). Thus, it is supported the continuation of Romania's participation in international formats that stimulate cyber-security debates (e.g., within organizations such as the UN, OSCE, NATO or EU). However, the component of formal and informal cooperation is presented too generally, given that the exchange of information between the public and private sectors is encouraged in order to mitigate cyber risks (ITU et. alii., 2021, p. 32), but that no mechanism or format of operational cooperation at the national level is presented. The only

element aimed at promoting the capacity for international cooperation refers exclusively to Romania's foreign policy in the field of cyber-security but excludes other areas of interest for such formats, such as arms control, trade or data protection, aspects desirable to be addressed, as specified in the ITU Guide (ITU et. alii., 2021, p. 53).

Results and Discussions

The numerical situation of the total, partial or non-fulfilment of the ITU recommendations can be found in Table 8.

Table 8: Summary representation of the fulfilment of the ITU recommendations, depending on the number of specific areas. (Source: author's view)

	Totally fulfilled recommendations (i.e., *present*)	Partially fulfilled recommendations (i.e., *partially*)	Not fulfilled recommendations (i.e., *unidentified*)
NCS UK	33	4	1
CS EE	22	13	3
SSCR RO	12	14	12

By exclusively referencing the ITU Guide and the 3 cyber-security strategies that were analysed, it can be concluded that NCS UK is the best correlated strategic document with the recommendations formulated by the ITU, and the SSCR RO the least. One of the possible explanations for this result lies in the number of cyber-security strategies adopted by each state until the present. The UK has so far issued 4 cyber-security strategies, Estonia 3 such documents (MAEC Estonia, 2019, p. 7), and Romania 2 (Romanian Government, 2022, p. 5).

Although the strategic vision assumed and adopted by the decision-makers at the level of a state is dependent to a large extent on the national context, the field of cyber-security is, on the one hand, multidisciplinary, and on the other hand in close connection with the events and debates carried out at regional and international level. For all 3 states, there are still a number of elements that are not satisfied or are partially satisfied in relation to the ITU Guide. However, our research has

highlighted that the United Kingdom and Estonia generally aim for strategic objectives for which there are already ongoing projects at the national level, while Romania encourages the development of such projects, but without presenting the existence of those already in progress or those planned. It is necessary for the future edition of Romania's cyber-security strategy to concretely capture existing projects and initiatives at the national level, meant to contribute to the achievement of the strategic objectives assumed.

Conclusion

The aim of this research was to highlight the common elements and the differences in the strategic perception of the field of cyber-security in the level of the United Kingdom, Estonia and Romania. Given that we have undertaken a descriptive and explanatory comparative analysis, by using ITU recommendations as an analytical grid, we have fulfilled the research objective. Although we have chosen the United Kingdom, Estonia and Romania for comparison, any other combination of three would have brought some relevant aspects for a national cyber-security comparative analysis. For future research, we believe that it could be useful to assess by comparison cyber-security strategies or polices form different international organisations or from much culturally diverse nations than the ones we chose.

References:

1. CCDCOE. (n. d.). Locked Shields. Retrieved February 8, 2022, from https://ccdcoe.org/exercises/locked-shields/

2. Council of Europe. (n. d.). *The Budapest Convention* (ETS No. 185) and its Protocols. Retrieved February 13, 2023, from https://www.coe.int/en/web/cybercrime/the-budapest-convention

3. DNSC. (n. d.). *Informatii generale despre NIS* (Legea 362/2018). Retrieved February 13, 2023, from https://dnsc.ro/pagini/informatii-generale-despre-nis

4. Estonian Parliament. (2015, January 22). *Penal Code*. Retrieved February 10, 2023, from https://www.riigiteataja.ee/en/eli/522012015002/consolide

5. European Commission. (2022, September 16). *The Digital Economy and Society Index – Countries' performance in digitisation.* Retrieved February 21, 2023, from European Commission: https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance

6. European Union. (2016, July 6). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN. Retrieved February 6, 2023, from EUR-Lex: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016L1148&from=RO

7. HM Government. (2022a). *National Cyber Strategy 2022*. Retrieved March 16, 2023, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

8. HM Government. (2017, September 11). *National Cyber Security Strategy 2016 to 2021*. Retrieved February 21, 2023, from GOV.UK: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

9. HM Government. (2022b, July 12). *Legislation to counter state threats*. Retrieved February 2, 2023, from https://www.gov.uk/government/consultations/legislation-to-counter-state-threats

10. Information System Authority. (2022, November 17). *IT baseline security system ISKE*. Retrieved February 8, 2023, from https://www.ria.ee/en/cyber-security/management-state-information-security-measures/it-baseline-security-system-iske

11. Information System Authority. (n.d.). *Monitoring cyberspace and impeding incidents*. Retrieved February 8, 2023, from https://www.ria.ee/en/cyber-security/handling-cyber-incidents-cert-ee/monitoring-cyberspace-and-impeding-incidents

12. ITU Development Sector. (2021). *Global Cybersecurity Index 2020*. Retrieved December 7, 2022, from ITUPublications: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

13. ITU et. al. (2021). *Guide to Developing a National Cybersecurity Strategy.* Retrieved March 16, 2023, from United Nations: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf

14. MAEC Estonia. (2019). *Cybersecurity Strategy. Republic of Estonia*. Retrieved March 16, 2023, from https://www.mkm.ee/media/703/download

15. Romanian Government. (2022, January 3). *E-monitor.* Retrieved February 12, 2023, from Monitorul Oficial: https://monitoruloficial.ro/Monitorul-Oficial--PI--2Bis--2022.html

16. Romanian Parliament. (2009, July 24). *Codul penal din 17 iulie 2009*. Retrieved February 13, 2023, from Portal Legislativ: https://legislatie.just.ro/Public/DetaliiDocumentAfis/223635

17. Romanian Parliament. (2023, March 15). *Monitorul Oficial*. Retrieved March 15, 2023, from https://monitoruloficial.ro/Monitorul-Oficial--PI--214--2023.html

18. Shafqat, N., & Masood, A. (2016). *Comparative Analysis of Various National Cyber Security Strategies*. International Journal of Computer Science and Information Security, 129-136.

INTELLIGENCE AND SECURITY IN THE 21ST CENTURY

THE IMPERATIVES OF RESHAPING THE NATURE OF INTELLIGENCE TO ADDRESS THE 21ST CENTURY SECURITY CHALLENGES

Ioana LEUCEA[*]
Adrian POPA[*]

Abstract:
Highlighted even in the Bible within the famous episode of liberation of Israelites from Pharaoh's slavery under the leadership of prophet Moses, intelligence as an action of collecting information about enemy for the purpose of creating an advantage for own side or as a way of fortifying own security has constituted a realm of ideas from immemorial time. Many scholars illustrated different examples and gave different reasons for researching the paradigm of intelligence yet the aspect less emphasized was the importance of connecting and discussing intelligence in relation with the effectiveness of diplomatic and military undertakings correlated to specific strategic cultural and geopolitical contexts. This paper discusses the importance of reshaping intelligence in accordance with the 21st century security challenges and indicates that intelligence should suffer profound transformations for the purpose of backing the settings of nations' foreign policies according to their desired geo-strategic status. Overall, intelligence might be nowadays the silver bullet reaching the minds of soldiers, society and policymakers for a secured world.

Keywords: *awareness, intelligence, security, strategy, warfare, 21st century.*

Introduction

The national and international security challenges manifest new dynamics, correlated with features of the social international arena emphasising themes such as classical military crisis, but also cognitive warfare, disinformation and propaganda (Mölder et. al., 2021). This

[*] Associate professor PhD, "Mihai Viteazul" National Intelligence Academy, Bucharest, Romania; email: leucea.ioana@animv.eu
[*] PhD "Mihai Viteazul" National Intelligence Academy, Bucharest, Romania; email: popa.adrian@animv.eu

status quo generates serious impetus to reconsider the nature of intelligence, its role, functioning and all its correlated features. Yet the contemporary security challenges gives no time to procrastination but to formulate theoretical answers having great practical relevance when considering the actionable intelligence.

The classical perspective of intelligence as a complementary area of study offering an upgraded understanding of international relations, extremely fascinating for scholars, policymakers and the general public has now very important practical ends.

Its mirage derives not only from the variety of theories and conceptualizations, but also from the mysterious side of one of the most secretive and less researched areas of international relations that do not longer represents the "opium of the intellectuals" (Aron, 1955) but the main cognitive battlefield projecting the future of international society. Indeed, the theoretical answers the scholars provide, even within the field of intelligence studies, take part in the global competition for cultural lenses the people use and act upon.

The aim of this paper is to offer an overview of intelligence concept, based on historical and theoretical aspects derived both from ancient philosophers and modern scholars, for the purpose of depicting the development of the intelligence paradigm and not ultimately, to highlight through relevant examples that the classical assumptions on the role of intelligence might be outdated in connection, for instance, with the effectiveness of diplomatic and military undertakings.

Theoretical background

Intelligence along with its multitude of features was an encrypted paradigm both in theory and in practice despite its ancient background. Although organised intelligence and its emergence as a sub domain of international relations are relatively new, intelligence is one of the oldest professions that transcend time since antiquity. However, as an old saying reveals, longevity does not automatically mean understanding.

"Questions like what is intelligence?", "What does it do?", "What should it do?", as well as discussions over the possible answers have included professors, students, independent scholars and intelligence practitioners. "They have informed a growing number of articles,

conference panels and anthologies. These debates have indirectly influenced policy" (Warner, 2014, p. 25).

Michael Herman (2007, p. 9) has argued that intelligence – a set of permanent institutions – dates back only to the second half of the nineteenth century, but as information and new (intelligence) has always been collected as part of warfare (…) and equally important in peacetime. Related to the idea of cognitive or hybrid threats, the classification of intelligence as a set of permanent institutions might be unessential in the contemporary context within the endeavour to respond to asymmetric treats that might require the involvement of the entire society.

The same judgement may be formulated when speaking about the role of spies. The role of espionage was perceived during history as extremely relevant, the specialists insisting on the idea that espionage was used starting with unmemorable times. This aspect has been also outlined by the aforementioned author: "rulers from the earliest times tapped the knowledge of merchants and other travellers" (Herman, 2007, p. 9).

The insistence on the idea that there were many contributors to the adjustments of the intelligence paradigm who were aware of the importance of this tool for the policymakers, from its primary status to its institutionalised emergence, has persisted in the public narrative.

One of the earliest consecrated authors who wrote about intelligence in terms of gathering information about enemy for the purpose of obtaining a strategic advantage in military decisions was no other than Sun Tzu, an ancient Chinese military general who authored the famous book *The Art of War* – considered to be fundamental for the theory of military strategy. For instance, in the last chapter of his book, *On the use of spies*, Sun Tzu develops ideas that reveal his awareness on the direct causality between accurate intelligence and the efficiency of a military undertaking.

Indeed, foreknowledge – understood as knowledge or awareness of something before its occurrence –, is highly appreciated by Sun Tzu (1998, p. 168) who argues that it "cannot be gotten from ghosts and spirits, cannot be had by analogy, cannot be found out by calculation; it must be obtained from people, people who know the conditions of the enemy".

Furthermore, Sun Tzu (1998, p. 172) emphasizes the importance of espionage in times of peace or war as "is essential for military operations, and the armies depend on this in their actions". In this way, the typology and the profession of spy started to make career in literature.

However, in the context of the 21st century security challenges, the typology of the profession of spies fades away as the enemy has no longer definite and identifiable contours. As Fred Schreier (2010, p. 37) outlines, the new threats have ubiquitous profiles, amorphous design and "are increasingly transnational, non-conventional, and asymmetric in nature…are more random and non-linear in emergence, almost impossible to predict in advance, rendering foreknowledge of intentions, doctrine, and rules of engagement most difficult to obtain". Indeed, countering the new threats requires intelligence to be more related with the original idea of intelligence: intelligence as information.

Another illustrative ancient philosopher who tackles this topic is Sun Bin, a descendant of Sun Tzu's philosophy school. Sun Bin advances the idea of studying intelligence, moving the thematic from security dilemma to strategic advantage (*shi*) reasons. According to translators of Sun Bin, D.C. Lau and R. Ames (2003, p. 63) "when *shi* is translated as strategic advantage, many Western readers move immediately to assign it to one side of the conflict or the other. *Shi*, however, refers to all of the factors on both sides of the conflict: numbers, terrain, logistics, morale, weaponry and so on".

In addition, D.C. Lau and R. Ames (2003, p. 63) remark that Sun Bin emphasizes "that *shi* is not a given, but it must be created and carefully cultivated". Cultivation through education and the rewarding of people who gather information, the spies, is one of the key actions in achieving military success. This opinion is shared by Sun Tzu (1998, p. 170) who admitted that "therefore no one in the armed forces is treated as familiarly as are the spies, no one is given rewards as rich as those given to spies, and no matter is more secret than espionage." As it can be noticed, these classical approaches outline once again that accurate intelligence plays a decisive role in the effectiveness of diplomatic and military undertakings.

Departing from the ancient times and reaching the middle Ages, we encounter the work of another philosopher that devoted important part of his research to understanding the secrets of war and subsequently, the advantages of accurate intelligence. Florentine statesman, writer and political theorist, Niccolo Machiavelli analysed the spectrum of intelligence within the only theoretical work printed during his lifetime, The *Art of war*. The aforementioned author gives advice regarding the avoidance of betrayal, so numerous within the conflicts of the dark ages: "if you suspect anybody in your army of giving the enemy intelligence of your designs, you cannot do better than to avail yourself of this treachery by seeming to trust him with some secret resolution which you intend to execute, while you carefully conceal your real design; hence, you may perhaps discover the traitor and lead the enemy into an error that may possibly end in its destruction" (Machiavelli, 1965, p. 170).

Practically, Niccolo Machiavelli offers a brief idea over the cure against betrayal, being a primary definition for the use of counterintelligence as a way of assuring successful military or diplomatically undertakings. In addition, the Florentine statesman illustrates different hypostases when intelligence combined with strategy play an important role in military actions: "in order to penetrate the enemy's secret designs and to discover the disposition of his army, some have sent ambassadors with skilful and experienced officers in their train dressed like the rest of their attendants (…) others have pretended quarrel with, and banish, a particular confidant who has gone over to the enemy and afterward informed them of his designs. The intentions of an enemy can also be sometimes discovered by the examination of the prisoners you take (…) but above all things, a general ought to endeavour to divide the enemy's strength by making him suspicious of his counsellors and confidants" (Machiavelli, 1965, pp. 171-173).

Therefore, Niccolo Machiavelli offers not only strategic advice regarding military movements or positions, but also his work is related to previously mentioned Sun Bin's *shi*, being focused on acquiring strategic advantage through using intelligence and counterintelligence. The interpretation of the aforementioned author reveals the importance

of counterintelligence for the information warfare: identifying the strategic narratives enemies would employ to convince the audience to act in accordance with the strategic output envisaged. The strategic advantage of intelligence when speaking about cognitive warfare gets decisive importance when correlated with strategic communication and persuasion as reaching the mind and soul of the opponents is a *sine qua non* imperative.

According to Cambridge dictionary, intelligence means "secret information about the governments of other countries, especially enemy governments, or a group of people who collect and deal with this information" (Cambridge Dictionary, 2022). However, definitions of intelligence are rarely offered by scholars due to the ambiguity of multiple possible conceptualizations and the complexity of the strategic environment which configures and establishes the component parts that are encompassed within this theoretical puzzle generated by the connections with the enemy`s strategic objectives.

In the spirit of this statement, James Der Derian (1992, p. 19) admits that "intelligence is the least understood and most under theorised area of international relations" and here we find the explanation: the strategic map or environment. However, one of the most frequent definitions of intelligence belongs to M. Turner (1991, p. 303): "information management: gathering raw information; analysing it; and disseminating evaluated information to decision makers, some of whom have been elected to make national security decisions".

The modification of the accent in the definition of intelligence might be that related to decision makers as in a democratic political culture or context the intelligence dissemination has the society or the general public as beneficiary. Therefore, the interpretation offered by James Der Derian (1992, p. 21) as "intelligence is the continuation of war by the clandestine interference of one power into the affairs of another power" can be interpreted as well as cultural intelligence or cultural diplomacy.

Indeed, the relevant information to be transformed in intelligence has very strong connections with strategy. A certain strategic culture is involved when an actor assumes that, for instance, the last (but not the least) stage of the "cycle of intelligence" is constituted by the

dissemination process. Delivering the best truth to decision makers might have marginal importance when the instruments of influence in a cognitive battlefield are for instance fictional information based on soft power means used for the purpose of reaching certain strategic or political goals.

Therefore, defining intelligence requires correlation with certain strategic cultures, strategic objectives and temporal fragmentation or historical periodization. As Jennifer Sims (2014, p. 45) concluded, "intelligence cannot be reduced to a fact-checking service and still succeed at enabling competitive wins." Finally, having in mind the need to better understand the tendency highlighting the accent put on the collection stage of the intelligence cycle in correlation with the spectrum of the 21st century security challenges, the authors consider that intelligence should be re-evaluated in connection with the strategic outcomes to be accomplished using intelligence means.

Beneficiaries and critics

It is a well-known fact that US president gets a daily overview on intelligence whereas British Prime Minister receives regular reports. The content of information received by political leaders is extremely important because their decisions are weighting enormously and as a consequence, intelligence obtained should be carefully filtered through all component stages before dissemination.

However, intelligence failures can occur for many reasons and at any stage of the intelligence cycle and not infrequently the consequences are extremely serious; for instance, different warnings received from intelligence agencies before the launch of the terrorist attacks of 9/11 or 7/7 were not sufficient in order to thwart the plot.

Despite the commonality within scholars and public regarding the benefits of the intelligence for society in general and for political decisions in particular, there is still reluctance regarding the actionable or practical aspects of intelligence. Indeed, the intelligence paradigm has raised several questions within the public for different issues such as transparency, hidden funding, violations of human rights or famous failures. However, it should be remarked that some of these issues are

generated by mass-media whose perspectives are not all the time the most researched.

As it is known, failure attracts more attention than success not only because of the audience of the 21st century, so much interested in presumably never seen subjects, but also because successes are mostly kept in quiet as a possible foreign interference can alter the *modus operandi*. Michael Herman (2007, p. 224) argued that "the circumstances of intelligence increase the risk of biased judgements about it. Its failures make for good media exposure; and official enquiries always search for culpability, in a way historians are liable to inherit (…) for example, the USA's effective use of Western intelligence on Soviet military preparations to deter Soviet action against Poland in 1980-1 has attracted less attention than the failure to judge that the Warsaw Pact preparations around Czechoslovakia in August 1968 were for a military invasion."

However, sometimes an outcome of an intelligence operation can be dualistic, different perspectives being perceived depending on the subjectivity of the commentator. Michael Herman (2007, p. 225) contextualizes this idea with much ability "the Cuban missile crisis was partly an intelligence failure, since US intelligence originally discounted the possibility that Soviet surface-to-surface missiles would be deployed on the island. Yet their subsequent detection in U-2 imagery was an intelligence triumph."

The input of the intelligence agencies for the diplomatic and military undertakings

Agencies are different from state to state as their orientations are shaped by different geo-political characteristics. James Rusbridger (1991, p. 37) offers a unique characterisation of the most dominant intelligence agencies: "Americans like their billion-dollar computerised organisation, believing that big is beautiful, and now these monoliths are out of control. The British stumble after Americans trying to copy their technology but waste their limited resources because their agencies are run by an amateurish elite who are too highly politicised and target the wrong enemies, allowing the real spies to go free. The Russians are so bureaucratic that any gems of intelligence they might cull are lost in a

mass of trivial dross. The French are pragmatic to the point of openness over their illegal activities but in the end, it is the smallest and most immoral of them all, Mossad, which is the most efficient." (James Rusbridger, 1991, p. 37)

A possible counterexample for the impact of intelligence on military and diplomatically decision resides in Mossad. This secret service is extremely efficient as combines the efficiency of a small group of dedicated agents with the advantages of an ethnic and religious community of Jews all over the world who are serving the cause of Israel from minor arrangements such as shelter or food for agents to counterintelligence. James Rusbridger (1991, p. 37) remarks that "whether any intelligence does much good or actually enhances a country's security is doubtful. After all, despite the success of Mossad, Israel still lives in a perpetual state of fear and terrorism. But the intelligence game is now an international affair where winning and point-scoring is the most important thing". Certainly, a good intelligence cannot be the guarantor of a nation's security, but more than sure it is involved in a high degree.

Again, the reshaping of intelligence in accordance with the strategic goals within an international dynamic context is of highest importance. Defining intelligence in an ahistorical perspective might have no relevance as a toolkit for mapping its role in a fundamentally changed environment. As Jennifer Sims (2014, p. 46) put it, intelligence should be related to international politics. Indeed, intelligence favours the settings for nations' foreign policies according to their geo-strategic status.

Nowadays, intelligence sharps its surveillance skills and warning methods to counter-act even newer threats such as terrorism. Intelligence is important in terms of prevention as it functions as a surveillance mechanism ready to intercept through counter-espionage any threats to the national security. Espionage is also an intelligence tool heavily used in both peacetime and wartime and it can vary from technological, economical to military purposes.

An interesting passage, very relevant in understanding the reasons of espionage, is depicted in the book *Red Horizons*, written by Lieutenant General Ion Mihai Pacepa, the highest-ranking intelligence official ever to have defected from the former Eastern Bloc. In the context

of rememorizing a meeting with the Romanian dictator Nicolae Ceausescu where different *intelligence thefts* from Western countries were presented to him, Ion Pacepa reveals the following dialogue: "Weapons, comrades, are the most desirable items of trade in today's world. That does not mean we shouldn't also smuggle plain chips out onto the Western market as American-made (Ceausescu) and a high rank intelligence officer replied "we haven't spent any money on research" and "we haven't paid for the license". We don't have to pay any royalties. And our labour costs are a fraction of those in the West. It wouldn't surprise any of us to see some "Western firms in trouble soon" (Pacepa, 1987, pp. 46-47).

As a consequence, not only that espionage can be cost-effective in terms of expenditure, but it can also create a strong imbalance in terms of economic, military and technological equity. Indeed, intelligence theft was an intensive and common procedure of during the Cold War, and this practice is still topical nowadays.

A huge number of attempts or accomplished intelligence thefts are reported yearly through mass-media or government release. Most common intelligence thefts are conducted by geopolitical enemies or in other words, challengers, but sometimes intelligence smuggling happens within allies. James Rusbridger (1991, p. 36) chose a relevant example in order to illustrate this aspect: "Despite the fact that over the years America has been Israel's guardian, both politically and militarily, and continues to give Israel $3 billion-worth of aid annually, that does not stop it from falling victim to Mossad's activities. In 1985, Jonathan Pollard, a US Navy analyst, was paid $30,000 by Mossad in return for handing over thousands of pages of top-secret material. As part of the same operation, Mossad is credited with the theft of enough uranium from a plant in Pennsylvania to make six nuclear weapons." (James Rusbridger, 1991, p. 36)

Talking about the imperatives of intelligence, Michael Herman (2007, p. 155) concludes that: "its effect is to optimize national strength and international influence, on varying scales (…) In both war and peace intelligence's consistent impacts are cumulative, relatively unsurprising contributions to effectiveness and influence. Overlaying any regular patterns there is serendipity or luck.

Conclusions

The nature of intelligence theme has a preeminent importance at the global scale. The fact that intelligence concept does not have a fully-covered theoretical background highlights the importance of correlating and embedding it within the concept of strategic environment or international political culture.

Policymakers realised the importance of accurate intelligence in their militarily and diplomatically undertakings as its effects have emerged in a variety of fields of action such as: army, technology, cybernetics or diplomacy. As a result, intelligence remains a persistent priority of governments. Therefore, the intelligence paradigm attracts the interest of scholars, policymakers, philosophers and the general public as it developed and amplified the agenda of security culture. The mirage of this paradigm comes from the mystery that surrounds this subject. More common under the auspices of covert operations, intelligence has a huge impact on the diplomatically and militarily undertakings.

As a consequence, what intelligence represents has become not only a subject to explore for mainly theoretical ends, but the very important asset in order to achieve and accomplish the task of providing security in a world deeply modified considering the parameters used in mapping the international security environment.

In the context of the 21st century challenges, it is critical to understand intelligence by employing adequate hermeneutics of facts. As in the traditional positivist concept, intelligence is supposed to deliver "facts" and "not diverge into assessments and other kind of guesswork", there is a wonder whether even "the standard model of the role of intelligence in decision-making" will still be based in the future on this image of an "idealized policy expert" bringing neutral authority to bear on policy (Marrin, 2009, p. 135).

Therefore, the legends surrounding intelligence will always be attractive as we are keen to know what "the other" thinks. The mentality of "the other is nowadays more than ever targeted, the interests and the counteracting measures continuing to be searched for". Whereas successes of intelligence reflect in our daily lives, astonishing failures will always make big echoes in our minds.

References:

1. Aron, Raymond. (1955). *The Opium of the Intellectuals*, Routledge, New York.

2. Bin, Sun. (2003). *The art of warfare*, State University of New York Press, Albany.

3. Cambridge Dictionary, *Intelligence,* accessible online on http://dictionary.cambridge.org/dictionary/british/intelligence_2 (accessed 10 January 2023).

4. Derian, James Der. (1992). *Antidiplomacy: spies, terror, speed, and war*, Blackwell Publishers, Cambridge.

5. Herman, Michael. (2007). *Intelligence power in peace and war*, Cambridge University Press, Cambridge.

6. Machiavelli, Niccollo. (1965). *The art of war*, Da Capo Press, New York, 1965.

7. Marrin, Stephen. (2009). *Intelligence analysis and decision – making. Methodological challenges*, in Gill, Peter, Stephen Marrin & Mark Phythian, (2009). "Intelligence Theory. Key questions and debates", Routledge, London & New York.

8. Mölder, Holger, Vladimir Sazonov, Archil Chochia, Tanel Kerikmäe (eds.). (2021). *The Russian Federation in Global Knowledge Warfare. Influence Operations in Europe and Its Neighbourhood*, Springer.

9. Pacepa, Ion Mihai. (1987). *Red Horizons: chronicles of a communist spy chief*, Regnery Gateway, Washington D.C.

10. Rusbridger, James. (1989). *The Intelligence game: Illussions and delusions of international espionage*, I. B. Tauris & Co Ltd Publishers, London.

11. Schreier, Fred. (2010). *Transforming Intelligence Services. Making them Smarter, More Agile, More Effective and More Efficient, Study Group Information*, Schutz & Hilfe, Vienna and Geneva.

12. Sims, Jennifer. (2014). *The theory and philosophy of intelligence*, in Dover, Robert, Michael Goodman & Claudia Hillebrand, *Routledge Companion to Intelligence Studies*, London and New York, Routledge.

13. Tzu, Sun. (1988). *The Art of War*, Shambhala Publications, Boston.

14. Warner, Michael. (2014). *Theories of intelligence. State of the play*, in Dover, Robert, Michael Goodman & Claudia Hillebrand, *Routledge Companion to Intelligence Studies*, London and New York.

STRENGTHENING THE SECURITY CULTURE IN ROMANIA

Bianca-Elena STAN (PREDOANĂ)[*]
Ana-Rodica STĂICULESCU[*]
Marius-Răzvan PREDOANĂ[*]

Abstract:
The current security context requires proper and consolidated solutions in order to lower the number of risks posed by the ongoing national security threats. Strengthening the security culture is one of these solutions, as it can ensure the engendering of desirable attitudes towards existing security risks. Shortly, security culture is a combination of knowledge and attitudes toward the security issues of the state. In Romania, since 2010, the consolidation of security culture is an assumed objective within the National Defence Strategies. Over time, different Romanian institutions have taken several steps to achieve this goal, but a main actor is represented by the Romanian Intelligence Service, as it took multiple measures in order to have a better-informed population and better trained authorities. In addition, the National Cyber Security Directorate has been actively involved in strengthening the cybersecurity culture, an extremely important branch of the security culture. Taking into consideration that every human activity is more and more connected to the cyber space, people have to face many risks coming from this direction.

In this article you will find information about some measures taken in Romania in order to strengthen the security culture. The main objective of this article is to emphasize the importance of creating a common security culture, but also to spot the limits of such a process. For accomplishing this objective, it was used "literature review" as a research method.

Keywords: *security culture, strategy, risks, defence, training.*

Introduction

What is security culture? Why is it important? What are the benefits brought to the state and to its citizens? What are the tools of

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

Romanian authorities for strengthening the security culture? All these questions represent the main objectives of this article, along with the desire to make a topic that lacks public attention more visible, even though it is of a great importance: security culture. The research method used was "literature review" by integrating multiple data from different findings and perspectives.

Security culture is a new concept that incorporates various meanings from a micro environment to the state or interstate level. This can be considered a branch of national and universal culture, but it becomes more than that, as it is a vital dimension for the strategic leadership. Security culture refers to a set of knowledge and attitudes towards the security issues that a state face. So, the purpose of the security culture is to help the citizens of a society to be aware of the potential dangers and to encourage them to participate in the process of achieving national interests. The security culture is rather an ongoing process, because the knowledge fund needs to be constantly updated and connected to the dynamics of the regional and global security environment.

Snyder (Ustun, 2010) defines security culture as a set of ideas, emotional answers and patterns of behaviour that members of the national strategic community acquired through training, imitation or exchange of knowledge on strategies. So, Snyder focuses his definition on security culture at a managerial level. This level is essential, preliminary, in the process of consolidating security culture among population.

More recently, Chiru (2016, p. 65) defines security culture as an "interrelated set of information, values, attitudes about security, which shapes security behaviours of social individuals, including perceptions of security risks."

Why is security culture important?

The post-Cold War era brought a significant shift in the use of power, from the hard power (military) type, to the soft one, which focuses more on the economic level. This shift has also led to considerable changes in the "war" meanings. Today, "war" has a new content and several forms of manifestation. Decreasing trust in the state institutions, declining social cohesion and denying national values can be

new forms of an unseen war, a slow one, whose battlefield has become invisible. Unfortunately, the changes brought by the end of the Cold War cannot be stopped, diminished or excluded. Also, the forms of manifestation of future threats cannot be anticipated, but preventive measures can be taken in order to ensure the continuity of the state, even if society faces black swan scenarios.

In this security context, raising the security culture among population (and especially among the leading factor) might be a useful prevention measure. The security culture must provide the individual with a complex ability of understanding a large spectrum of security issues – from how their own computer can be used by another person thousands of miles away to carry out a cyber-attack, to the advantages and disadvantages of using shale gas (Munteanu, 2013). The security culture is an absolutely necessary pillar, also because of the fact that it determines favourable attitudes and behaviours that lead to individual and state security.

Security culture meets the following specific goals and needs followed by the leading factors that have responsibilities in the security field (Piwowarski, 2017):

a) effective control of high-risk and high-impact threats;
b) recovery of security in case of imbalances generated by different events;
c) optimizing the different levels of security understanding;
d) increasing individual and social awareness of the need for trichotomous development (mental/social/material).

According to Ioan Deac (2018), the security culture defines the group identity of a community/society and it ensures social solidarity around common goals that inspire devotion, loyalty, cohesion, sense of belonging and patriotism. Therefore, the security culture provides the implementation of a well-structured set of values, both within a social group and, also, at the individual level. This is utterly important, as values will directly influence the adoption of certain future attitudes. The attitudes will guide the individual's behaviour towards action/active involvement and in this way, society will finally have responsible citizens that take part into the national security ongoing process.

In a more theoretical approach, we can say that security culture brings its contribution through the functions that it possesses (Onișor, n. d.), which are often related to stability, integration and continuous progress.

The informative function ensures the population's general information regarding the security system structure, the political actions of its components, the national and common/collective security values (Onișor, n. d.). This function builds knowledge about the institutions responsible for national security, the inter-institutional cooperation, as well as the actions taken by them in order to ensure a safe environment. Moreover, the informative function creates a framework of the values and norms concerning individual and state security, which can influence desirable behaviours. This function develops in two directions, from the power factor to the population, but also from the population to the ruling class. This way, all the involved actors benefit from knowledge. First of all, the citizens are aware of the decisions taken by the rulers, as well as the basis on which they were developed. Next, the rulers are informed about citizens' choices, interests and grievances and about the ways their messages and actions are perceived. This set of data is extremely relevant as it could anticipate attitudes and behaviours on social, security and political issues.

The axiological function of the security culture points out how security values are perceived in connection with international politico-military phenomenon and, also, the concrete ways of establishing values in a national system (Onișor, n.d.). Through this function, a set of opinions, beliefs and ideas about security values are formed. These can generate acceptance, attachment and involvement or, on the contrary, indifference and rejection. Furthermore, these approaches lead to certain attitudes towards political and the security events that take place inside and outside a state, attitudes that can facilitate or hinder the governing process. Therefore, the security culture is an indispensable factor for the state stability, due to the fact that it creates a strong link between society and the ruling class.

The normative function refers to the way security values become norms, procedures, rules, techniques and security standards meant to give stability to the state and to ensure the state's contribution of the

international security (Onișor, n.d.). Besides these norms, the attitudes of the citizens are of great importance, but especially the attitudes of the institutional apparatus that must guide the citizens through own example. If the rules are not followed by those who drafted them, it will generate disobedience and indignation. It is essential that the rules and regulations governing internal and international security be accepted by a clear majority of the population, not only by a small community.

Thus, the security culture, through these three functions, provides a framework for the driving factor, but also an effective guidance to the citizens, as it offers a set of relevant information, attitudes and behaviours towards the state security.

Security culture – a strategic objective

The perception of risk is correlated with cultural factors, because the cultural models are those that establish a system of interpretation of facts and the attribution of emotions. In order for a whole population to have favourable, coherent and predictable perceptions and responses to a threat, it is absolutely necessary to create a common culture of security. One relevant and primary step towards this aim is represented by communication, especially, public communication on risks. An important channel is represented by official documents that stipulate current risks (for instance, the National Defence Strategy or other related documents).

The Guide of National Defence Strategy for 2015-2019 is an essential document that defines the steps which should be done for consolidating the security culture in Romania, both at the institutional and societal level. According to this document, the process involves a joint effort of society and institutions with responsibilities in the field of national security. The role of institutions is to ensure that the rights and freedoms of every citizen are respected, while the role of society is to inform and to provide institutions with relevant directions concerning all identified issues. The Guide mentions the definition of security culture in accordance with this approach: "a concept related to the need to learn generating security, both as a citizen or as a state" (Presidential Administration, 2015, p. 14).

The Guide promotes a public communication between citizens, organizations and institutions in the field of national security. As this

communication can only be shaped throughout a solid security culture, there were identified several steps for its consolidation (Presidential Administration, 2015):

- encouraging citizens to develop a security culture with the help of media products and other various related ways;
- introducing security culture in the education field through courses, conferences and so on;
- creating and promoting different informative materials;
- training security experts;
- continuous collaboration with national and international organisations that aim to strengthen the security culture.

For a proper communication it is imperative to be productive in the following three dimensions (Sandman, 1988): 1. Experts and society; 2. Experts and decision makers; 3. Decision-makers and society. It is, also, important how communication is carried out. Its content must be clear and concise, in order to be correctly received by the interlocutor. Possible distortions, generated by own interpretations of the content, can alter the message and, consequently, change the perception and attitude of those who receive it.

Consolidating the security culture in Romania

The Romanian strategic documents establish that security culture needs a joint effort made by both civilian and military institutions and also a continuous effort for raising awareness among population. The intelligence services are also responsible for promoting a security culture among population, because such a concept would ease their dialogue with citizens and other institutions of the state. No human being is born with a set of clearly printed instructions, so it is necessary to promote precise rules, regulations and values throughout effective informing channels and a better transparency of the institutions responsible for national security.

The Romanian Intelligence Service attaches great importance to strengthening the security culture, using various training methods, such as: meetings with civil society representatives, debates, conferences or various partnerships with academic or research institutions (Calangea, 2017).

The opening of Security Culture Information Centre (RIS, 2003) was an important step in fulfilling the mission of the Romanian Intelligence Service within the National Plan for Romania's Accession to NATO, Chap. IV, regarding the creation of a security education. This centre has led to increasing public communication and much more effective training of the citizens in relation to the security environment.

The Security Culture Information Centre was inaugurated on September 30, 2003 and it provides an organized framework for debating security environment issues. The "Security Culture" pilot program is addressed to students, researchers, the academic world, journalists and all those interested in the promotion of security culture and Euro-Atlantic values. Through this program, it is created a database consisting of studies, researches and reports of national and international organizations. This database must be available to the public and the debate groups that operate within the Centre.

Other relevant actions taken by the Romanian Intelligence Service in order to promote the security culture are (Calangea, 2017):

1. The campaign „Terorismul de lângă noi" ("The terrorism near us"). It took place between 2004 and 2010 and its purpose was to raise awareness among pupils, high school students and, last but not least, representatives of public authorities about the terrorist threat and its implications. The campaign was really useful in consolidating relevant knowledge in this field.

2. The international conference „Tu poţi preveni terorismul" ("You can prevent the terrorism", 2007). It took place at Cluj Napoca County Library and aimed to present the steps taken by the Romanian Intelligence Service to prevent and combat terrorism.

3. The round table conference „Societate, Democraţie, Intelligence" ("Society, Democracy, Intelligence", 2008). Its purpose was to identify the perceptions of population towards the Romanian Intelligence Service actions, but also to assess the need to strengthen the public relations regarding the area of intelligence.

4. „SRI în 50 de minute" ("SRI in 50 minutes", 2013) was a 50 minutes informative session that provided data on the security environment, as well as data about the proper ways to manage the security risks.

5. The debate „Evoluţii social media: o privire spre viitor" ("Social media evolutions: a look to the future", 2015) which focused on the new risks determined by the growing influence of social media on the public relations.

6. The master's degree program „Studii de Securitate – Analiza Informaţiilor" ("Security Studies – Information Analysis") offered by the Faculty of Sociology and Social Work of the University of Bucharest. It aims developing analytical skills among master students, as well as creating a strong security culture.

7. The international conference *Intelligence in the Knowledge Society* – organized annually by the "Mihai Viteazul" National Intelligence Academy in order to exchange experiences and good practices in the intelligence area among doctoral and postdoctoral students from Romania and abroad.

8. The student scientific communication session ANISTUD – organised, also, by "Mihai Viteazul" National Intelligence Academy for both civilian and military students. It promotes the share of knowledge and opinions through debates on various topics in the area of national security and beyond.

9. The journals – *Intelligence*, as well as Romanian Intelligence Studies Review are, also, important steps in consolidating security culture among society, as they provide essential knowledge in the field of national security and generate transparency of Romanian Intelligence Service and its activities.

10. The Romanian Intelligence Service online activity is, perhaps, the most powerful tool for increasing the security culture, because everyone is connected to the digital environment, so this way it is created a direct communication channel with people. The Romanian Intelligence Service has developed friendly web design websites, such as: sri.ro, animv.ro, intelligencestudies.ro or intelligence.sri.ro. Also, the Romanian Intelligence Service has an active presence on social platforms, including: Facebook, Instagram, Twitter and YouTube. Open-Source Intelligence (OSINT) plays an essential role in creating the security culture, as it constantly identifies the needs for change and adjustment of the Service's approaches in accordance to technological and social developments.

11. The Romanian Intelligence Service runs an awareness program, designed to raise awareness of risks, vulnerabilities and threats among employees of companies of strategic importance, but also among civil servants. Through this program, the Romanian Intelligence Service aims highlighting the main risks generated by the access to certain data; training these professional categories in order to adopt a counter-informative behaviour; emphasizing the importance of self-protection (Romanian Intelligence Service, 2017).

12. The Romanian Intelligence Service has carried out a campaign among high school and college teachers in order to help them identify possible cases of radicalization among young people. Once identified, teachers can report those behaviours or even help treating them. Strengthening the security culture among teachers represents an important measure, as teachers can pass on the knowledge to students and create security education among them.

In order to consolidate the security culture at the experts' level, there were also promoted many prevention and intervention programs for the representatives of the Romanian institutions (Romanian Intelligence Service, 2016):

- RAN (Radicalization Awareness Network) – it was developed in 2011 at the European Union level, with the participation of experts in the field of radicalization, among NGOs, academics or police and intelligence services.
- CoPPRa (Community Policing Preventing Radicalization) – it was created in 2010 within the European Union to train police officers in detecting radicalized persons. Personnel from the Romanian Intelligence Service, the Ministry of Internal Affairs and the Ministry of Justice also took part in this program.
- CLEAN-IT ("Fighting the illegal use of the internet with public-private partnerships from the perspective of counter terrorism") – it is a program developed by the European Commission in 2011 and our country is part of it. It is aimed to develop a set of rules and good practices that would stop the use of the Internet in carrying out terrorist activities.
- PLIR ("First Line Against Radicalization") – it is a program developed in 2014 by the Romanian Intelligence Service along

with the Ministry of Internal Affairs, being an extension of the CoPPRa program at the national level. Its purpose is also to train police officers to identify radicalized people.

Besides, the Romanian Intelligence Service pays close attention to the cybersecurity culture, as it became one of the most important parts of the security culture. According to the Service official website, any person is exposed to cyber risks, but the main targets are represented by the Romanian state institutions (SRI, 2018). However, even when it comes to institutions, the main vulnerability is represented by people, because nowadays everyone manages IT&C systems. Therefore, the representatives of the Romanian Intelligence Service argue that every citizen must be aware and understand the need to secure and protect their own computer systems. In order to raise cybersecurity culture among the citizens, the Romanian Intelligence Service has carried out the next measures:

A. Cybersecurity Good Practice Guidelines – taking into consideration increased exposure to cyber risks determined by the society's constant connection to cyberspace, the Romanian Intelligence Service has issued a cybersecurity guide. It is addressed to every citizen and can be found on the official website of the Service.

The guide is an important source for strengthening the cybersecurity culture, as it gathers many aspects of cybersecurity (SRI, 2018):

- rules for safe Internet browsing;
- securing the Internet connection;
- multiple anti-malware protection;
- using a firewall program;
- rules for the protection of personal data;
- securing the use of e-mail address;
- tips for choosing a solid password;
- the need to periodically update the software;
- the periodic backup;
- tips for securing access to the Wi-Fi network;
- rules for the protection of personal data during travels;
- recommendations regarding the use of social platforms.

In addition to these data, the guide includes useful tips for developing a cybersecurity culture within organizations (data about implementing an information security policy, defining responsibilities and properly integrating information security principles).

B. *Cyberint Bulletin* – since 2018, the Romanian Intelligence Service has published the *Cyberint Bulletin*, a biannual publication that aims to inform citizens about the trends in the field of cyber security. Its role is to summarize and present data about cyber-attacks, viruses, actors involved, good practices and so on.

C. Glossary of cybersecurity terms – the Romanian Intelligence Service (2019) has published a glossary of the most used terms in the field of cyber security. The glossary includes both basic and complex terms, explained through short definitions that can be understood by any citizen. Thus, it represents a good measure for increasing the knowledge field.

D. Carrying out the Awareness Program – as we mentioned earlier, the Romanian Intelligence Service has developed an extensive awareness program dedicated to relevant (national security related) entities from our country. The program aims to raise the level of awareness even in the cyber security field. Through this program, there are emphasised topics such as cyber-attacks, actors and defending methods (RIS, n. d.).

The National Cyber Security Directorate (NCSD – former CERT-RO) is also an active institution that fights for strengthening the cybersecurity culture among the Romanian society. The NCSD's publications, as well as the constantly organized events, contribute both to the education of the citizens and to the improvement of the employees with attributions in the cyber field. There have been identified the following NCSD activities:

I. Cybersecurity Weekly News and Cyber Risk Alerts – every week, on the NCSD website (www.dnsc.ro) are published the news in the cyber security field. The information is clear and summarized in order to offer to the readers the possibility to get informed quickly and correctly and, of course, to create over time a solid cybersecurity culture. In addition, NCSD has created a special section on the website, called THREATS, meant to warn the general public on the recent risks in the cyberspace.

II. Awareness campaigns – NCSD has conducted several cyber threat awareness campaigns over time. These focused on the following topics:

- malware on mobile devices;
- prevention of cybercrime among young people;
- fraud with false technical support.

III. Conferences – the annual conference "New global challenges in cybersecurity" was organised from 2011 up to 2020. It started with a small focus group of cybersecurity experts and later became the largest conference in the country, bringing together both public and private decision-makers on cybersecurity. In addition, the conference gained a global perspective, as speakers and participants from around the world were taking part. The themes focused on the new global challenges in the field of cyber security.

Another example is the international conference "Preventing and Combating Cybercrime" – organized in 2016 by the Faculty of Law of "Babeș Bolyai" University in partnership with NCSD and other organisations. The conference was attended by prestigious guests from 8 European countries, including the United States. The debates focused on the following topics: electronic harassment, cybercrime and prevention, property rights in cyberspace and so on (NCSD, 2016).

IV. Workshops for experts from public and private sector – NCSD in partnership with private institutions and companies has conducted over time multiple workshops dedicated to cybersecurity experts and to representatives of public institutions or private sector:

- workshop dedicated to a next-gen endpoint protection product (NCSD, 2017);
- workshop dedicated to SSL solution – "visibility and Data leak prevention (DLP) Network Monitor" (NCSD, 2017);
- workshop dedicated to server security and cyber threats prevention (NCSD, 2017);
- workshop dedicated to proper managing of WANNACRY attacks (NCSD, 2017);
- workshop dedicated to "Smart WIFI and Cloud Managed LAN & WLAN" (NCSD, 2017);

- workshop dedicated to protection of industrial control systems (NCSD, 2017);
- online workshop dedicated to the Connecting Europe Facility (CEF) Telecom program (NCSD, 2020).

V. Target group training sessions – NCSD organized a cyber-security course for Agerpres journalists (NCSD, 2016). The purpose of this program was to bring awareness about cyber-attacks, actors, as well as useful data about safety rules. The journalists took part into a practical demonstration in order to measure their awareness of cyber threats. For a better understanding of the cyber risks, NCSD simulated a cyber-attack.

NCSD specialists took part into the "European Judicial Cooperation in the field of combating cybercrime" project (NCSD, 2016). They carried out a training program for the judges and prosecutors (Romanians and Bulgarians) in the field of cybercrime. The program focused on cooperation in the fight against cybercrime at the European level.

All these steps taken by the Romanian Intelligence Service and NCSD are a proof that security culture represents an important pillar both at the societal and the institutional level. Besides these, the desire for transparency and the constant public communication are also relevant steps for the process of consolidated security culture, because it leads to a closer relationship between society and the state institutions and create a better understanding of the needs of population.

Limits of the security culture shaping process

The process of consolidating security culture among society is as useful as it is costly and difficult to achieve. Thus, we must consider the main limitations in the process of shaping the security culture.

First of all, an efficient communication from leaders to population requires the use of a very large accumulation of financial, material, human and time resources. Top-down communication from government to society must be a continuous and transparent process, which is utterly difficult to achieve. It is well known that this type of communication can often lead to distortions or filtered information, caused either by internal factors, related to the individual, or by external ones such as press or public relevant actors. Media can generate own interpretations or even create conspiracy theories in order to attract the citizens to a certain

part. It must be taken into consideration that disinformation can be created not only into our country borders, but also outside of them and the limits in stopping such messages are a lot. The right to free speech, as well as the inability to cover permanently such a wide range of information are worth mentioning.

Secondly, strengthening the security culture requires a very well organized and explicit framework of security values, norms and rules. It is true that all these are mentioned in the official strategic documents, but the way they have been transposed, as well as the low visibility in the public area, made these efforts unknown to the ordinary citizen.

Third, the security culture involves a constant "look" at the ruling factor. As long as the leader is not a role model that respects and promotes the security norms and values, its credibility and legitimacy in front of population may be automatically lost. Not only that the leader won't be considered a trustworthy man, but his actions will be challenged and his decisions will be outrageous. Once a system has lost its credibility, it will certainly be ineffective in the process of strengthening a common security culture. Formed beliefs will always have an impact on the attitudes and behaviours of the majority, no matter how complex are the attempts of changing people's perceptions.

Last but not least, another factor that could hinder the process of shaping security culture is represented by the level of education among society. In order to base knowledge on security values and norms, it is essential to have a consolidated image on the country's general situation: inside situation and outside situation as a member of the international community. Having in mind these circumstances which can lead to an understanding of the need for values/norms and therefore to the adoption of certain decisions and behaviours.

Conclusions

Starting from the questions posed in the introduction of this article, we can conclude the following:

1. The security culture is a set of knowledge about the security risks, vulnerabilities and threats, as well as a set of desirable attitudes and behaviours for individual and state defence.

2. The security culture is an important pillar for the national security ensuring process, because it shapes the perception of reality (the perception of risk and safety), but also the attitudes of citizens. We can also assert that security culture is important, because it determines a more efficient communication between citizens and the responsible institutions in the field of national security.

3. In terms of benefits brought to the state and its citizens, security culture provides relevant benefits for the current security context.

First of all, the average citizen has a useful framework on the proper behaviours required for his own defence. For instance, a person with a strong security culture will know that using the same password for all the online accounts can generate major security risks in case of a cyber-attack.

As for the state, the security culture ensures a better cooperation with the citizens, which can be an extremely useful tool. A person with a strong security culture will understand much faster the security risks and will be more aware of the help they should provide to the responsible authorities. For example, if a regular citizen has information about what radicalisation means, in case he/she identifies any signs, it will certain that he will communicate those signs to the responsible authorities.

4. Even though the Romanian authorities have used numerous tools for strengthening the security culture, many of these have remained unknown to citizens. As we mentioned in this article, the security culture is a strategic objective for Romania, so the efforts to this direction must be considerable. Our country has included the consolidation of security culture in the strategic documents since 2010. Up until now, several steps have been taken in order to connect the population and the Romanian institutions to the ongoing security risks.

The Romanian Intelligence Service is one of the most involved institutions in this process. Over time, the RIS representatives held several events to increase awareness among the population (conferences, debates, presentations, informative sessions, student scientific communication sessions, journals editing, master's degree, awareness program, informative materials and so on). NCSD has also been actively involved in providing the population with useful information about cybersecurity, which has led to the strengthening of

cybersecurity culture (cybersecurity news, awareness campaigns, conferences, workshops, training sessions and so on). Both institutions have, also shown interest in training certain professional categories (their own staff, public servants, magistrates, journalists, and police officers).

Even if all these measures meant strengthening the security culture were not really in the public eye, they were important steps in achieving the strategic goal. Strengthening the security culture is not a simple process that is why there should be a constant awareness of the limits of such a process: distorted communication by various internal or external factors, a bad framework of security rules and regulations, a low level of education among population and so on.

References:

1. Buluc, R., Deac, I. & Lungu, C. (2018). *Promovarea Culturii de Securitate*. Bucureşti: Asociaţia ProSCOP.

2. Calangea, C.D. (2017). „Cultura de securitate. Surse şi resurse". *Revista Intelligence*. Accessed on 30.05.2022 from www.intelligence.sri.ro/cultura-de-securitate-surse-si-resurse/

3. Chiru, I. (2016). „Percepţia socială asupra riscurilor de securitate naţională: un ingredient (lipsă) al culturii de securitate". *Revista Cultură de securitate şi diplomaţie publică*, 16, 59-72.

4. Presidential Administration. (2015). *Ghidul Strategiei Naţionale de Apărare a Ţării pentru perioada 2015-2019*. Accessed on 15.06.2022 from http://old.presidency.ro/static/Ghid%20SNApT_2015-2019_AP.pdf

5. Romanian Intelligence Service. (2003). *Serviciul Român de Informaţii a inaugurat Centrul de Informare pentru Cultura de Securitate*. Accessed on 15.06.2022 from https://sri.ro/articole/serviciul-roman-de-informatii-a-inaugurat-centrul-de-informare-pentru-cultura-de-securitate

6. Romanian Intelligence Service. (2016). *Calendar Contraterorist*. Accessed on 30.05.2022 from https://www.sri.ro/assets/files/publicatii/CALENDAR_CT_2016_RO.pdf

7. Romanian Intelligence Service. (2017). *Awareness*. Accessed from https://www.sri.ro/awareness

8. Romanian Intelligence Service. (2018). *Ghid de bune practici pentru securitatea cibernetică*. Accessed on 16.06.2022 from https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf

9. Romanian Intelligence Service. (2019). *Glosar de termeni pentru domeniul securității cibernetice*. Accessed on 15.06.2022 from https://www.sri.ro/assets/files/publicatii/GLOSAR-TERMENI-CYBER-12-09-2019.pdf

10. Romanian Intelligence Service. (n.d.). *Cyberintelligence*. Accessed on 30.05.2022 from https://www.sri.ro/cyberint

11. Romanian Intelligence Service. (n.d.). *Awareness*. Accessed on 15.06.2022 from https://www.sri.ro/awareness

12. Munteanu, R. (2013). *Importanța culturii de securitate în mediul dinamic al globalizării*. Accessed on 16.06.2022 from https://adevarul.ro/international/in-lume/importanta-culturii-securitate-mediul-dinamic-alglobalizarii-1_517e5993053c7dd83f5a0cd2/index.html

13. NCSD. (2016). *Conferința Internațională "Preventing and Combating Cybercrime" (20-21 Mai 2016).* Accessed on 30.05.2022 from https://dnsc.ro/citeste/preventing-and-combating-cybercrime-2016

14. NCSD. (2016). *Curs de securitate cibernetică la AGERPRES*. Accessed on 26.06.2022 from https://dnsc.ro/citeste/curs-de-securitate-cibernetica-la-agerpres

15. NCSD. (2016). *CERT-RO sprijină pregătirea magistraților pentru combaterea criminalității informatice*. Accessed on 15.06.2022 from https://dnsc.ro/citeste/cert-ro-sprijina-pregatirea-magistratilor

16. NCSD. (2017). *Workshop de prezentare a unei tehnologii de tip next generation endpoint protection.* Accessed on 30. 05.2022 from https://dnsc.ro/citeste/workshop-bitdefender-gravity-zone-elite

17. NCSD. (2017). *Workshop de prezentare a soluției SSL – visibility and Data leak prevention (DLP) Network Monitor.* Accessed on 16.06.2022 from https://dnsc.ro/citeste/workshop-combridge

18. NCSD. (2017). *Workshop de prezentare cu privire la securitatea serverelor și prevenirea atacurilor cibernetice*. Accessed on 15.06.2022 from https://dnsc.ro/citeste/workshop-anssi.

19. NCSD. (2017). *Workshop pe tema bune practici în gestionarea atacurilor de tip WANNACRY*. Accessed on 30.05.2022 from https://dnsc.ro/citeste/workshop-pe-tema-bune-practici-in-gestionarea-atacurilor-de-tip-wannacry

20. NCSD. (2017). *Workshop CERT-RO – Combridge: soluții de securitate pentru Smart WIFI și Cloud Managed LAN & WLAN*. Accessed on 17.06.2022 from https://dnsc.ro/citeste/workshop-cert-ro-combridge-

21. NCSD. (2017). Workshop on *Protejarea sistemelor de control industrial*. Accessed on 30.05.2022 from https://dnsc.ro/citeste/workshop-pe-tema-protejarea-sistemelor-de-control-industrial-

22. NCSD. (2020). *CERT-RO organizează un workshop online de prezentare a programului Connecting Europe Facility (CEF) Telecom*. Accessed on 15.06.2022 from https://dnsc.ro/citeste/cert-ro-organizeaz-un-workshop-online-de-prezentare-a-programului-connecting-europe-facility-cef-telecom

23. Onișor, C. (n.d.). *Contribuții Teoretico-Metodologice privind Cultura de Securitate.* Suport de curs înregistrat în Biblioteca Centrală Universitară a ANIMV, București.

24. Piwowarski, J. (2017). "Three Pillars of Security Culture". *Security Dimensions International and National Studies,* 22, 16-27. Accessed on 16.06.2022 from https://www.researchgate.net/profile/Juliusz_Piwowarski2/publication/323243164_Three_Pillars_of_Security_Culture/links/5a883550458515b8af91b64f/Three-Pillars-of-Security-Culture.pdf?origin=publication_detail.

25. Sandman, P.M. (1988). "Risk Communication: Facing Public Outrage". *Revista Academică Management Communication Quarterly*, 2, 235-238.

26. Ustun, C. (2010). *Turkey and the European Security Defence Policy*. New York: Tauris Publisher.

HISTORY AND MEMORY IN INTELLIGENCE

MOTIVATION FOR INTELLIGENCE-SERVICE WORK – THE GERMAN DEMOCRATIC REPUBLIC STATE-SECURITY

Helmut MÜLLER-ENBERGS*

Abstract:
Though the interest in the motivation behind intelligence work is great, hardly any empirical investigations have been published. This may be due to the subject itself being difficult to research. Intelligence services, secret police and the police hardly report openly on such matters, especially considering their reluctance to expose their conspiratorial personnel in academic investigations. Included in the findings published by "experts" are mostly testimonials and evaluations from criminal proceedings involving informers, which, under empirical aspects, hardly lead to valid results. The group of defendants poses only an exposed minority, presumably aware of its advantage in criminal law, and consequently unlikely to venture more "primitive" motives. The greater number of testimonials, mostly communist and post-communist memoirs, is similarly unhelpful since the former agents, messengers or spies emphasise their ideals as motivation. In contrast, the confidants tending towards materialism report less openly about the structure of their motivation.

Keywords: *Ministry for State Security, agents, scouts, spies, unofficial collaborators, motivation.*

Introduction

Principally, the intelligence services and the police search for their candidates at best in, or in close contact to groups of their interest, in order to "break them out" or smuggle them in. The disposition, the presumed state of motivation of the target-person is to be estimated in every case and calculated during the first interview. The state-security of

* Dr. phil., professor at the Center for Cold War Studies at Syddansk Universitet (Denmark), 1992 - 2019 research assistant at the Stasi Documentation Authority (now the Federal Archives), 2015 - 2021 head of counterintelligence in the state of Berlin.

the GDR collected extensive information about a candidate in a formally defined process (called "Aufklärung"), in order to arrange a competent and reliable recruitment. This could be completed in a shorter time, but usually took a year or more. It did not depend on the candidate himself or his actual necessity alone, but also upon the degree of his freedom to decide whether he should cooperate or not. This obviously undermines the unproven empirical presumption that idealism is seldom found in criminal investigations, though practically always amongst dissident agents. This motive is more often suspected in recruits and members of the army than in prisoners, but even less in the rest of society.

Motivation is different when the consideration of advantages is involved. These may have been stronger in prisoners as in agents. Consequently, **prisoners will have been forced to collaborate more often than agents, who could always avoid such pressure**. Based on this assumption, the types of motive for intelligence-work revealed through the influence of imprisonment, the army, society and dissidence should each be separately considered.

Motives of prisoners

Candidates awaiting trial and those in prison had the least scope for making decisions. They were completely dependent upon the goodness of the warders, police, state-security, judiciary and, possibly, interrogators of the GDR. The basic interest in improved prison conditions, daily advantages, an earlier release or proportionally milder sentence, simplified the recruitment of possible informers who were called, in this microcosm, "unofficial contacts," or, "cupboard-agents," or, "cell-informers," or – from co-prisoners' point of view-, "Zinker," (zincer) with reference to criminal secrecy or, "Zellenrutscher" (Cell slide)[1].

The department IX of the Ministeriums für Staatssicherheit (Ministry of Sate Security, now foreword MfS) which was responsible for the cell-informers amongst prisoners awaiting trial, availed of a net of almost 200 unofficially employed prisoners – regarding the number of prisoners as a whole, a substantial proportion. On average, there were four to seven prisoners per "Zelleninformator" (ZI) – subversive

[1] All the translations are the author's unless otherwise noted.

collaborator (hereafter SC). This level of "saturation" was intended. At least one SC should be operational in every working-place and every sleeping-area, in all workshops and teams. Preferably, convicted criminals were to be mobilised. In the year 1987, 15 to 22 SC's were recruited (Müller-Enbergs, 2008, p. 317 and 321). During the late eighties, 68 % of the cell-informers were used for up to three months, 21 % up to six months and 11 % for over twelve months.

The fluctuation of the cell-informers was remarkably high, being subject to releases, amnesties and exposure of conspiratorial connections. Eleven per cent refused to continue with their cooperation for personal – "security" reasons. Their being in contact with the MfS in prison, posed a high personal and physical risk, since exposure by co-prisoners was likely, and the resulting sanctions were severe.

Only one investigation into these motives exists to date. It was prepared by the state-security. The department IX of the MfS reported in 1987, of the 166 recruited cell-informers, 55 % admitted that "reparations" motivated them to cooperation, especially through the withdrawal of applications for emigration (Müller-Enbergs 2010, p. 87). In 40 % of the cases the central consideration was of personal advantages, especially in expectation of earlier release from prison, and 5 % attached their readiness to cooperate with the hope of permission to leave for West Germany (Beleites, 2001, p. 131; Erdmann, 1998; Müller-Enbergs, 2010, p. 87).

In the prisons of the GDR in the '80s there were, on average, about 33.000 prisoners (Werkenthin, 1995, p. 408), whose unofficial infiltration was considerable. Tobias Wunschik was the first to investigate the motives of prisoners for subversive cooperation using established empirical material, but was unable to define the connection between the motive-groups. The central theme was a lighter or a shorter sentence, including more bearable positions within the works-management and, for example, the occasional material bonus of a packet of tea. Wunschik did not find evidence of ideational motives, as was apparent in the '50s amongst communist prisoners (Wunschik, 2003 and 2012). The few statistical reports on the motives of prisoners awaiting trial, permit conclusion that **psychological pressure and personal gain were instrumental for the cooperation with the state-security.**

Motives of recruits and relatives of the army

Within the MfS, "Hauptabteilung I" was the department responsible for the recruits and the relatives of the "Nationale Volksarmee", the Army. The 2.300 full-time staff was responsible for the personal and functional security of management, troops and all facilities, not only of the army, but also of the border patrols of the GDR. Furthermore, the responsibility of the staff covered the Ministry for National Security and its own facilities. In addition to this, came the task of espionage in the Bundeswehr (Army), the Bundesgrenzschutz (Federal Border Guard) and the Grenzpolizei (Border Police) (Wiedmann, 2018, p. 217). With approximately 22.000 subversive collaborators, the department controlled 13 % of the SCs of the MfS. The scope between collaboration and refusal, concerning subversive involvement during military service in the GDR, especially in the "Volksarmee", could not have been great. Leadership qualities were in high demand since the military had to be ready for battle 85 % of the time. The intelligence work was done in close contact with the military hierarchy. Soldiers' career-options and improved service conditions were promoted by cooperation with the state-security. Nonetheless, leading a SC life was just as difficult as it was in the prisons. Conspiracy at the meetings in barrack-conditions was difficult, because the members of the MfS were well known. Whilst on duty, a SC would not be able to leave the military base without permission, for meetings outside the base he would require a leave- permit or holiday-permit, and would have to register out. This also applied to officers. There was also the problem that the SCs had to seem respectable amongst their comrades, which hindered them in collecting valuable information about irregular behaviour. If they showed difficult behaviour, their career-options may have been limited. With regard to conscription, the MfS tried to engage young SCs beforehand, as it was practically impossible during the 18-month duty period. The conspiratorial work of most of the SCs ended with the completion of their conscription, partly because the local section of the MfS no longer required them, and partly because they were no longer willing to continue the work. **The proportion of ideational motives will probably have been more poorly represented for exactly this reason.**

Motives for subversive work in everyday life in the GDR

At the MfS own law school, "Juristische Hochschule" (JHS) – the Secret Service School, at Golm-Eiche near Potsdam, in the department, "Politisch-operative Spezialdisziplin", the employees had a chair of psychology at their sole disposal (Moritz, 2017). Research made by the JHS in the year 1973 with the title, ***The Recruitment of Subversive Staff and their Psychological Requirements*****, emphasised the increased importance of the "use and development" of SC-candidate and SC motives (**Korth, 1973**).**

The investigation involved was concentrated mainly with the preventative work of the MfS, the area of work, operating primarily within the GDR, and listed the motives, called here, **"Reasons for Recruitment", in three complexes: conviction, needs and interests as well as blackmail ("making amends").** The complex, conviction, was subdivided in the investigation into Marxist-Leninist, patriotic, humanistic, religious, moralistic and anti-capitalist conviction.

Positive models were given and used as examples for SC work. The needs and interests' motive were diversified partly into material and social, and partly intellectual interests. The complex concerning blackmail was called, "the reparation and secure continuation – effort", or recruitment "under pressure", as mistakes by individuals were not reasons for punishment, but for compensation, following cooperation (Korth, 1973, p. 583).

Although the MfS abided by this rather stiff framework, it developed a delicate evaluation in differentiating between the individual motives. If the practical intelligence work with compromising information had a high status in the '50s and '60s – almost as high as political conviction – it disappeared in the following years in favour of material gain. This may, according to the authors of the above-mentioned investigation, not be immediately presumed to be a morally inferior, but rather a stronger motive. This research and the SC guidelines themselves also point out correlation and development of individual SC motives. Lastly, it was desirable to be able to claim political conviction as the basis for cooperation in SCs.

The job of the managing officer, or the leading SC member, also included establishing psychological characteristics of SC-candidates,

which could lead to motivation. After the candidate was chosen, he was subject to a series of tests on suitability, honesty and reliability. The more precise the confirmed information about the motives for collaboration was, the more likely a successful recruitment would become. Although this routine command of SC-testing by an organisation like the MfS seemed to be binding, it was obviously deviant when put into practice. Having studied archive procedures, the authors of the same research concluded that merely 15 % of the cases were founded on the judgment of reliability and honesty. Only 34 % showed SC-candidates' own willingness to cooperate. Moreover, 80 % of the assessments listed objective factors without even beginning with the subjective requirements. The analysis of documents regarding SC-candidates who refused to cooperate, showed that 35 % of the cases under examination lacked "possibilities for persuasion" in the personal details. Here the "politically ideational reputation" and the "knowledge of objective irregularities" were all that was to found from which uncertified conclusions could be drawn. This, though, seems to have been normal practice.

It is certainly of great interest to establish how closely related, the differing SC motives were. This query cannot be answered without involving the state-security. A remarkable dissertation from 1967 in ministry archive material, brought this complex to light in an empirical investigation (Hempel, 1967). The theoretical frame of this dissertation refers to the psychology of motivation from Hans Thomae (Thomae, 1965, pp. 3-44), with which it is sporadically, but not continuously comparable with the outlined concept. **Even if the results of the dissertation cannot be confirmed – the number of investigated cases is not mentioned – the listed results correspond with the modern process of evaluation. A questionnaire was developed for the actual MfS examination and presented before a "representative selection" of SCs in the regional management in Potsdam.** Asked about the major components of persuasion of SCs – it was possible to give several – 60.5 % named "recognition of social expectations" and, at any rate, 49.1 % "moral compulsion and moral constraint". Personal gain was named by only 27.4, "practical goals" by 39.9 and "self-satisfaction" by

11.9 %. "Threats and blackmail" were named by 23.4 % of those questioned, as a convincing motive (Hempel, 1967, p. 83).

So, the greater number of those questioned claimed that "politically ideational factors" were decisive in the subversive collaboration. Nonetheless, the proportion of "threats and blackmail"-cases were considered to be "surprisingly high", in that 22.1 % of those questioned included it as a secondary component. Accordingly, by almost every second person tested, anxiety, fear, stress and inhibition occurred at being asked to participate in subversive collaboration, also affecting behaviour (Hempel, 1967, p. 85).

Furthermore, it was clear from this survey that there are significant differences between the motives of men and women, just as there are between different age-groups. Even professional employment did not seem to be the fundamental influence on the nature of motivation.

Other results are listed concerning the party-political connections. Members of the SED or block-parties, recognised in 83 and 55.5 % respectively, the "social necessity"; 68.5 % of the recruited SED members and 42.1 % of the block party members felt a sense of moral duty and a compulsion of conscience, to work in collaboration with the state security. Amongst the recruited non-party members, these components were less distinct with 41.2 and 31.2 % respectively. The conclusion is: "Positive political and moral attitudes and loyalty to the socialistic society" promote, and "anti-social efforts" to gain personal advantage, hinder decidedly the existence of the subversive collaboration. "Negative political and moral attitudes, however, have the opposite effect" (Hempel, 1967, p. 94)

The connection between the nature of the recruitment and the motive is shown in the following results: where compromising material was used, 54 % claimed the threats and blackmail-motive to be the main component, just as 62.5 % of those asked about materialist interest. At the same time, 62.5 % of those persuaded by political conviction claimed the recognition of a social necessity (Hempel, 1967, Bd. 1, 97; Bd. 2, 6).

In the investigation, the question also arose, as to whether the reasons for recruitment had changed. The answers showed that "during collaboration, the motives of the unofficial collaborators change

substantially". Where, earlier, 60.5 % had claimed "recognition of a social necessity" as the main component of persuasion, 78 % did so at the time of the investigation. On the other hand, "personal profit" sank from 27.4 to 21.6 %, and "threats and blackmail" from 23.4 to 12.6 %. Though, "self-satisfaction" increased conspicuously from 11.9 to 25.4 %. This was explained by the fact that "the conspiring manner of the work somehow causes temptation and the interesting atmosphere, the extraordinary" emotional side-effects are "really experienced in many cases and consequently have a positive influence on the behaviour towards the state-security divisions during the probationary period." (Hempel, 1967, p. 101) As the cooperation continued, to follow suit, the frequency of the motives shifted to reasons of a singularly social connection: 50.2 % of the SCs asked, had doubts at the beginning of their unofficial collaboration, whereas 44.4 % had none. At the time of the investigation though, the number of doubters had sunk to 28.6 %, but those without doubt had risen to 68.7 %. Therefore, "substantial changes" had appeared during the unofficial collaboration, wherein the explanations and directions of the SC-managing staff play "the biggest role".

The dissertation concludes that "the research into the recruitment of the unofficial staff should be a continuous task accompanying the process of cooperation. The detailed evaluation of current motives and moral values and their development, in every case, is necessary in order to adopt changing characteristics in tasks of leadership and counselling. These changes should be considered in the delegation of tasks and the calculation of future behaviour." (Hempel, 1967, p. 164)

It is clear that ideological motives for subversive work predominated in GDR daily life, especially in respect of the quoted investigation, despite material interests and threats having been reported. Nevertheless, some questions remain unanswered: why does a husband report about his wife, whom he loves, to the state-security? Is it right to presume that this SC's patriotic motivation was worth more to him than his love for his wife? Or was he trying to protect her from prospective "danger" in connection with his work as a SC? Greater depth into the disciplines of psychology and sociological and philosophical insights, it seems, would be necessary in order to answer these questions. The discussion concerning these disciplines must be handled separately.

Motivation for Espionage

The greatest imaginable freedom, in avoiding recruitment by the state-security, could only be had by citizens outside the GDR. In the FRG, the under-cover work was mostly controlled by the "Hauptverwaltung A" (HV A), the department of the state-security responsible for espionage. The research into motives leading to cooperation between a West-German and the HV A or within a feigned personal relationship with ulterior-motive, ought to have belonged, as already mentioned, to the most important aspects of the examination during recruitment. The HV A always assumed a collection of differing motives ("motivational structure"), which were subject to change, but its regulations still followed the usual schematic portrayal of the MfS. The nature of the "recruitment guidelines" had changed.

Considering the latest state of affairs in December 1988, the HV A had the following picture of its active sources and subversive collaborators in the FRG and in West-Berlin: 60 % had agreed to cooperate for reasons of "politically ideational conviction" and 27 % on materialistic grounds (Müller-Enbergs, 2011, pp. 134-138). In 7 % of the cases, the deciding factor first named, was personal affection for the contact-person. Less than 1% was recruited, according to the "questionnaire statistics", under threat. In addition, 4 % were recruited under "foreign-flag", which may be relevant concerning the personal relationship, but not necessarily concerning the motive (Müller-Enbergs, 2011, pp. 134-138). This information from the documents of the HV A hardly concurs with the reports made by dissidents and former SCs. According to Friedrich-Wilhelm Schlomann, the Ministry for the Defence of the Constitution of 1960, relying on known cases, assumed that 43 % of the SCs had collaborated under "threat", 34 % for "personal gain", 14 % for "ideological conviction" and 7 % from a "thirst for adventure" (Schlomann, 1984, p. 87). The former spokesman for the Ministry for the Defence of the Constitution, Richard Gerken, wrote, quoting "official sources", that 70 % of the East-German recruitments made in 1965 were due to "threats", 25 % in hope of "business prospects", 2 % after being "led astray" (under foreign-flag) and 3% based on "political motives" (Gerken, 1965, p. 61). The power of the statements in these analyses, however, is reduced in that only the findings of exposed subversives

were considered, who may have been persuaded to make favourable testimonies, credible to the officials. In this respect, the evaluation of these statements should be critical.

Non-material Motives

The recruitment on the basis of "politically-ideological conviction" counted in the HV A as the main method in the '50s. It should have been voluntary, since this was seen as the safest basis for successful cooperation with the HV A. Even so, the scope for "conviction" was already so broad that it included non-Marxist orientated persons. It sufficed to correspond in part to stipulations in claiming "keeping the peace, fighting against atomic-death, against fascism or militarisation". The aim was, of course, to convince SCs motivated in this way, of the "superiority of the socialist position" (Müller-Enbergs, 2011, p. 301), as the subject was dropped in the new regulations of 2/68. Then the impression given by the student-movement, convincing in its negative stance to politics in capitalistic states, was accentuated, as well as the simple corroboration, "principally or part", with the "peace-politics" of the "socialistic camp" being brought to the fore (Müller-Enbergs, 2011, p. 359). At the last, in the final valid regulations of 2/79, all that was mentioned was "progressive political conviction", which included "all political opinions and stances" in which the "politics, institutions and representatives of the particular state were principally or partially rejected. The rejection could ("can") also express agreement, "principally or partially", with the politics of the socialist states. The expression "progressive conviction" embraced Marxist-Leninist, humanist through to apparently anti-imperialist attitudes. Further intentions accepted, were "love of peace, solidarity with oppressed peoples, patriotism and civil-democratic and humanistic efforts" (Müller-Enbergs, 2011, p. 57). The high number of SCs registered at the HV A on the grounds of "conviction", is considered to be unrealistic by the West-German office for the defence of the constitution. It seems this assessment should be reviewed. Indeed, the HV A did not assume, as did the West-German office, that the recruits acted out of "ideological corroboration (…) with the GDR-system" (Meier, 1992, p. 183). The argument that no material

means changed hands in only the fewest cases, does not necessarily indicate the lack of non-materialistic motives, as will be discussed elsewhere.

The "significant" motive of the danger of war grew in strength with the stationing of mid-range missiles. The "most effective motive" for subversive work was still the Marxist-Leninist conviction. Karl-Wilhelm Fricke also assumes that the ideological component had increased in the eighties, in comparison to earlier years (Fricke, 1982, p. 150). The HV A plan included the extension of the Marxist-Leninist conviction, structurally incorporating the changeable nature of motives. Research was made, concerning the influence on the idea of socialism in SCs, for this purpose. Proven points of relevance were:

"1. The search for possible points of corroboration;

2. To clarify the extent to which this corroboration is sufficient and dependable, for willingness and operative activities;

3. To clarify whether this corroboration can be developed or extended, and how;

4. The consideration of the level of manipulation." (*Instructional material*, 1987).

The HV A found another form of corroboration in the fifties, as the hope of a unified German state had not yet been relinquished. It even added "nationalistic" views to "politically-ideological conviction". In this type of recruitment, the interests of the "German nation" were emphasised. The "national pride" of these, mostly "civilian"-influenced individuals, was to be respected, and they were to be treated with care, but the "political training" should not be neglected (*Instructional material*, 1987, 11 f.). Due to the reduction in political tension and the prospect of two nations in the seventies, the "nationalist"-component faded into the background, whereas its importance "diverging reactionary convictions and interests", in the regulations of 2/79, clearly grew. Recruitments based on this motivation, though, were no longer possible in established partnerships, as they had been in the fifties, but only in relationships purposely set-up in order to extract information ("foreign-flag") (Müller-Enbergs, 2011, p. 301).

Considering Personal Gain

Material and personal interests were usually involved in ideologically motivated recruitments, as was established by the HV A, and played a definite role in the structure of collaborator motivation (Müller-Enbergs, 2011, p. 454). The HV A followed the assumption that, "imperialism" turns "all material and moral values into consumer products", which it intended to exploit in two ways, as stated in its regulations of 1/59. Either, there were people in "financial difficulty", or deliberately manipulated "material dependency". Despite the "great possibilities", these "grounds for recruitment" had the disadvantage of SCs, acquired in this way, being able to "change sides for more money", which was to be discouraged through the direct employment of "fist-security" (information intended to be used for blackmail). At the same time, further grounds for cooperation were to be achieved through "political training" (Günther, n. a, p. 100). Friedrich-Wilhelm Schlomann conjectured in the early '80s, that recruiting on an "economic basis" may have been a successful method, though not often used (Schlomann, 1984, p. 88).

The HV A stuck to its concept in the regulations 2/78 and 2/79, even if its importance seemed to be fading. Now, the main objective was to differentiate between aspirations to achieve social status and personal expectations. "Material interests" now stretched from "meeting reasonable needs" to "pronounced plans for personal profit and abnormal demands" (Müller-Enbergs, 2011, p. 360). Schlomann included advantages for prisoners and ailing relatives in the GDR, where relaxed entry-permit stipulations would help, as suggestions for personal interest (Schlomann, 1984, p. 88). The assessment of "material interests" as a motive, changed in the '80s, or at least, adapted to practical experience. They were now considered to be the "driving force" and accepted as a "primary motive", throughout (Müller-Enbergs, 2011, p. 579).

The distribution of financial assistance within the HV A was closely connected to its function. A project-manager could sign for 1.000 DM and the director of the HV A or his deputy, 10.000 DM. Where expenditure was expected to be returned, the manager could authorize up to 18.000 DM a year in costs, and the director and his first deputy over 24.000 DM.

Blackmail

In the regulations of the HV A, "blackmailing" into subversive-work was never mentioned. The theme was self-consciously referred to, as the "basis of compromising material" or the "will to make amends", defined as "abuse of situations in the life of certain persons, known to us, but unknown to the public, the employers and relatives, whose exposure could badly damage or hinder the professional and social status of these people. Such situations were as follows: the intended or suspected speciality of the MfS; criminal deeds, tax-evasion, embezzlement or "serious moral affaires". Occasionally, they were manipulated to reach the necessary "level of dependency" (Müller-Enbergs, 2011, p. 454).

In the '50s and '60s, some were put under "pressure" because of their NS-history ("earlier" "criminal" activity), which was generalised in the regulations of 2/68 as "will to make amends". This recruitment-reason assumed such a "bad conscience" in the recruit, that he would have the will to "appease his personal guilt" with subversive work (Müller-Enbergs, 2011, p. 360). Later, this variant was used to convert foreign agents. In the regulations of 2/79, this recruitment-reason faded into the background and was reduced to the context of discussions concerning dissidence (Müller-Enbergs, 2011, p. 489).

The attempt to convert foreign agents

Normally, the MfS first attempted recruitment of "agents of enemy secret-services" or "organisations against peace", who had a background in intelligence work (Müller-Enbergs, 2011, p. 302). The term "Überwerbung" (lit. across-recruitment), was used in connection with volunteers as well as persons specifically chosen by the MfS (Müller-Enbergs, 2011, p. 363). The prerequisite for an "Überwerbung" was a thorough examination of the candidate, in order to find or create situations which would tie him to the HV A, and which would be highly compromising if ever exposed. The candidate, therefore, should not have any "real alternative" to subversive-work. The consequences of refusal were to be made clear to him during the examination, but also, if he showed willingness to cooperate, he would be asked to deliver confirmable intelligence information to prove his "honesty", (and to

stock up on "fist-security"). Apart from this blackmailing method, the HV A regarded the material and personal interests of candidates with a "reactionary attitude", as characteristic in an "Überwerbung" (Müller-Enbergs, 2011, p. 625).

"Foreign-flag" – a feigned relationships to serve intelligence-work

As the standing of "real socialism" deteriorated, the practised method of "malicious deception" of the SC through "foreign-flag" increased in importance. Although only about 60, 4 % of the West-German SCs counted by the HV A in 1987, were recruited in this way, it is assumed that this "art of mastery" had been extensively applied in the '70s and '80s. Indications are found in 36 such examinations in the "area of operations" in 1986. From the intended recruitments, 17, almost half, were to involve "foreign-flag" operations.

Conclusion

Apart from the differing levels of personal freedom, further motivating factors should be mentioned and closely examined. The structure of the SC motivation ought to be examined in its relation to professional or political sympathy or enmity to the state. The easiest procedure for the MfS, was to recruit targeted civil-servants. It was irrelevant how much time or effort was involved in subversive activities. The effort in serving at a secret address, taking incoming information to be passed on, is much less than the work of an agent hiding secret documents, photographing them, delivering the films and receiving and sending radio-messages. Presumably, the more effort the intelligence-work involved, the more ideological the driving force had to be. From the documents, the impression is apparent that – depending on the personality of the SC – there were inhibitions concerning information in the reports. There was not much willingness to report about people in close relationship, but otherwise there was no problem. Lastly, as suggested above, there is an historical change in the motivational positions, just as there is in the individually changing motives. These themes are still to be discussed.

References:

1. Johannes Beleites. (2001). *Schwerin, Demmlerplatz: Die Untersuchungshaftanstalt des Ministeriums für Staatssicherheit in Schwerin* [*Schwerin, Demmlerplatz: The detention center of the Ministry for State security in Schwerin*]. Schwerin: Dölling und Galitz Verlag.

2. Erdmann, V. (1998). *Die "Zelleninformatoren" in der Untersuchungs-haftanstalt der MfS-Bezirksverwaltung Halle (Saale)* [*The "cell informers" in the remand prison of the MfS district administration Halle (Saale)*]. Magdeburg.

3. Fricke, K. W. (1982). *Die DDR-Staatssicherheit. Entwicklung. Strukturen. Aktionsfelder* [*The GDR State Security. Development. Structures. Fields of action*]. Köln: Wissenschaft und Politik.

4. Gerken, R. (1965). *Spione unter uns. Methoden und Praktiken der Roten Geheimdienste nach amtlichen Quellen. Die Abwehrarbeit in der Bundesrepublik Deutschland* [*Spies among Us. Methods and practices of the Red Intelligence Services according to official sources. Counterintelligence work in the Federal Republic of Germany*]. Donauwörth: Auer.

5. Günther, H. (ohne Jahr). *Wie Spione gemacht werden* [*How spies are made*]. Berlin: Aufbau-Taschenbuch-Verlag.

6. Hempel, M. (1967). *Die Wirkung moralischer Faktoren im Verhalten der Bürger der Deutschen Demokratischen Republik zur inoffiziellen Zusammenarbeit mit den Organen des Ministeriums für Staatssicherheit (2 Bände)* [*The Effect of Moral Factors in the Behaviour of Citizens of the German Democratic Republic to Cooperate Unofficially with the Organs of the Ministry for State Security*]. Dissertation. Potsdam; BArch, MfS, JHS 21775.

7. Korth, W., Jonak, F. & Scharbert, K.-O. (1973). *Forschungsergebnisse zum Thema: Die Gewinnung Inoffizieller Mitarbeiter und ihre psychologischen Bedingungen* [*Research results on the topic: The recruitment of unofficial collaborators and their psychological conditions*]. In JHS (Ed.), 1973; BArch, MfS, JHS, 800/73.

8. Meier, R. (1992). *Geheimdienst ohne Maske. Der ehemalige Präsident des Bundesamtes für Verfassungsschutz über Agenten, Spione und einen gewissen Herrn Wolf* [*Secret service without a mask. The former president of the Federal Office for the Protection of the Constitution on agents, spies and a certain Mr Wolf*]. Bergisch Gladbach: Lübbe.

9. Michels, M. & Wieser, M. (2017). *From Hohenschönhausen to Guantanymo By. Psychology's role in the secret services of the GDR and the United States*. In "Journal of the history of the behavioural sciences", 54, p. 1-19.

10. Müller-Enbergs, H. (2010). *Inoffizielle Mitarbeiter des Ministeriums für Staatssicherheit. Teil 1: Richtlinien und Durchführungsbestimmungen*

[*Unofficial employees of the Ministry for State Security. Part 1: Guidelines and implementing regulations*]. Berlin: Christoph-Links-Verlag.

11. Müller-Enbergs, H. (2011). *Inoffizielle Mitarbeiter des Ministeriums für Staatssicherheit. Teil 2: Anleitungen für die Arbeit mit Agenten, Kundschaftern und Spionen in der Bundesrepublik Deutschland* [*Unofficial employees of the Ministry for State Security. Part 2: Instructions for Working with Agents, Scouts and Spies in the Federal Republic of Germany*]. Berlin: Christoph-Links-Verlag.

12. Schlomann, F.-W. (1984). *Operationsgebiet Bundesrepublik. Spionage, Sabotage und Subversion* [*Operational Area Federal Republic. Espionage, sabotage and subversion*]. München: Universitas.

13. Schulungsmaterial (1987). *Die Ansatzpunkte für die politisch-ideologische Arbeit zur Entwicklung des Sozialismusbildes von IM (Inoffiziellen Mitarbeitern) OG (Operationsgebiet)* [*The starting points for political-ideological work to develop the image of socialism of IM (unofficial collaborators) OG (area of operations)*]. 1987, BArch, MfS, BV Gera, Abt. XV, p. 282.

14. Thomae, H. (1965). *Die Bedeutungen des Motivationsbegriffes* [*The meanings of the concept of motivation*], in *H. Thomae (Ed.), Allgemeine Psychologie (Band II. Motivation)*, [*General Psychology* (Volume II. Motivation)], Göttingen: Verlag für Psychologie Hogrefe.

15. Werkenthin, F. (1995). *Politische Strafjustiz in der Ära Ulbricht* [*Political criminal justice in the Ulbricht era*]. Berlin: Christoph-Links-Verlag.

16. Wiedmann, R. (2018). *Die Organisationsstruktur des Ministeriums für Staatssicherheit 1989* [*The organisational structure of the Ministry for State Security in 1989*]. Berlin.

17. Wunschik, T. (2003). *"Zinker" und "Zellenrutscher". Die Inoffiziellen Mitarbeiter der Staatssicherheit im Strafvollzug der DDR ["Zincers" and "Cell Sliders". The Unofficial State Security Employees in the GDR Penal System*], in "Horch und Guck", 12 (3), p. 61-70.

18. Wunschik, T. (2012). *Die Untersuchungshaftanstalt der Staatssicherheit in Rostock. Ermittlungsverfahren, Zelleninformatoren und Haftbedingungen in der Ära Honecker* [*The State Security Detention Centre in Rostock. Investigation procedures, cell informants and prison conditions in the Honecker era*]. Berlin 2012 (BF informiert, 31/2012).

INTELLIGENCE, SECURITY AND INTERDISCIPLINARITY

WHAT IS COMMUNICATION AND WHAT IT SHOULD BE? PROBLEMS WITH MODERN PUBLIC COMMUNICATION

Matei BLĂNARU*

Abstract:
In regard to public and strategic modern communication, at least in one respect everybody agrees - there are serious issues and ever larger categories of population seem to be increasingly difficult to reach by official messages and narratives, there are increasingly numerous left and right radicals and consensus, social cohesion and trust in authority and institutions is ever decreasing not only in Romania, but throughout the Western world. Not to mention proliferation of fake news, disinformation and conspiracy theories. The simple question is "Why?" But, going a bit further, the subsequent question this analysis is asking is whether "Do we really care to know why or we do not?" Are we really ready to know why and to admit why? Or are we the senders of public communication, part of the problem, and not only the recipients, the lack of education, as we like to think, or just hostile entities like the Russian Federation or others? As Stănciugelu et al. (2014, p. 338) stated that: Have we not diverted from the status of public communication issued by an impartial sender, as theory states it should be?

Keywords: *disinformation, fake news, communication, sociological bias, ideology, superiority complex.*

Introduction

If different analyses of the questions "Why is this happening?", why is it that we are having such problems regarding public communication, regarding disinformation, regarding increasing public distrust, come with different answers, linked to the academic profile of each of the researchers, each of them having, of course, their own

*PhD student at the University of Bucharest and an associate researcher at the Center for Sino-Russian Studies, ISPRI-Romanian Academy; email: matei.h.blanaru@gmail.com

pertinent and rational arguments, this analysis will focus on an answer according to which the main problem appears to be of sociological origin. In other words, the main problems behind increasingly efficient disinformation campaigns, increasingly less efficient public and strategic communication campaigns are sociological in nature and are quite serious – bias is one of them. And the bias is all the more of a problem when, of course, it is not only that we may not realize it, but we may not even want to consider or admit it. We will provide many examples below. However, before addressing the main problems on the issue, we should first see what the current understandings of communication or public communication are.

Communication Perspective

What is communication? If we were to take a look at the etymological root of the current word, we find out that in Latin the word *communicare*, among other meanings, also meant *to unite*, *to connect*.

What is public communication? Pierre Zémor, a well-known theoretician on the subject, says that: "public communication is formal communication which converges on exchanging and sharing public information and maintaining the social bonds, whose responsibility lies on public institutions" (Zémor, 2003, p. 27). So, social cohesion is one of the essential objectives of public communication, of public institutions, and we will ponder on this issue.

But which are the effects of public communication? Bernard Miège (Miège, 2000, pp. 75-78) considers there are four categories of effects that are usually sought after through public communication:

1. modernizing the way administration's function;
2. changes of behaviour in citizens (for example, wearing the safety belt);
3. building a modern image for some institutions or administrations;
4. seeking approval from citizens on certain issues (Bernard Miège himself says about this effect that "it is based on arguable principles (…); it is hard to accept that this communication would fall into public communication; it

> belongs to political communication (with the one exception that financing is… provided by SID)" Bernard Miège goes on to cite Jürgen Habermas who says that this function actually means publicity implemented exclusively in relation to the imperatives of manipulation. (Miège, 2000, p. 78) Thus, it is actually an effect filled with negative implications.

Nowadays, we have to ask ourselves whether we, as senders of communication, are still following the basic objectives and principles of public communication, which are information and social cohesion, or we are actually following other objectives while pretending to still care for the main purposes stated above – because all of these actually have an overwhelming impact on both the results of the communication act, and especially on our entire society.

What is strategic communication? If we were to synthesize a number of definitions mentioned here (Cornish, Lindley-French, Yorke, 2011, pp. 3-5), strategic communication would mean public communication which follows and supports accomplishing strategic objectives, identified here as primarily national objectives, but they can also just as well be political, economical, organizational or military objectives etc.

Which are the goals of StratCom? We cite some of these goals as they are mentioned in an analysis here (Mârzac, 2019, p. 2): "At a national level, StratCom has two objectives and values. On the one hand, to consolidate the nation through a common inspired idea, lasting and strategic, as a long-term platform for the strategy and the national strategic objectives. The same, it can strengthen cooperation and cohesion at a government and society level in accomplishing strategic goals. At the institution level (ministries, armed forces, police), StratCom is an instrument of organizational development which answers at questions like "why do we have armed forces?", "which values does the Ministry of Defence add to society?", "how is the Internal Ministry providing human security" etc. – problems linked to the fundamental objectives of government organizations. So, once again we have social cohesion and building trust in institutions, an objective somewhat subordinated to the first one. And although the way in which strategic communication is used differs a lot, just like the objectives in mind, the

main goals need to be these two: cohesion and building trust. But modern European and Romanian societies seem to show that we are somehow failing at acquiring both cohesion and trust. The current analysis tries to offer an answer to the question "Why is that?"

What Communication Should Be. Issues. Just as Pierre Zémor (2003) said, cited above, communication should be centered on the citizen, on unifying a society and on information, otherwise we leave a lot of room for fractures in the society. This is an elementary conclusion, well-known to anyone interested in public and strategic communication. Regarding these fractures, we may find it easy to point out that the Russian Federation is exploiting and enlarging them, but it is much more difficult for us to admit that it may be us who are causing them, in the first place.

How did we do that? It is simple – by using our public communication to push into a corner, to push away, to antagonize on purpose or not large segments in the population, at a European level, segments in population that some thought might not be "educated enough", "not modern enough" or not "progress-centered enough". So, what do we want to do with these large segments in the population deemed "uneducated", "unmodern" or "not progress-minded"? A question that was surely asked in certain circumstances, but nevertheless a question that should have never been addressed like that in a multidimensional, diverse society, centered on mutual understanding and recognition, and, it should have never been even thought like that.

Why? Because we must never start from the assumption (which is common to all ideologies) that "we are the ones who are right and everyone else is wrong and it is in our mission to 'enlighten' them all." What do we do with the ones who do not want to be "enlightened"? History gave us grueling examples of what happened in circumstances like that. And it is in our duty to represent all, our duty is to be the representatives of the society, to watch over its well-being, and not at all to be modern "apostles" of an ideology or another. However, unfortunately, this is the feeling given by most public communications at the European level, when dealing with societal aspects, societal

projections, public policies or the future of a society, just the same as in Romania.

How did we push people into a corner? We are interested in public discourse, public narrative that one too many times has assumed the role of forming opinions on ideological basis instead of trying to form a unity, a social cohesion. We talk a lot about cohesion, but the public narrative seems to address only some people, as if this cohesion is meant for some, but not for the others, which actually leads to a blatant contradiction. And, in the end, we should not be at all surprised to see that we have exactly the results that we sought after – ideological leveling and radicalization on the one side, and marginalization, pushing away, antagonizing and radicalizing maybe an even larger segment of population on the other side.

And one more important idea here, we should not fool ourselves at all, this is exactly the way in which we are fully contributing to weakening our society not only by the lack of unity inflicted (which leaves a lot of room for proliferation of hostile actions), but also by losing a lot of valuable members of our society who do not feel at all represented by public discourse and, thus, refuse to get involved in public institutions and in society with their full potential. What do we do, do we "despise" them, do we treat them with superiority as if we were self-sufficient, from the "heights" of our moral ideological perspectives that we deem to be a priori faultless, as if we did not need them at all? Do we really believe we do not need them? Because this is how many of them feel. This would be a big mistake that would cost us all a lot, but this is how many times European and national public communication feels like.

Examples. In order to try and give an example of what we mean, there was a famous interview (Alexandru M., 2021) when segments of the population that disagreed to Covid vaccination and other measures were called "terrorists". Afterwards, many people were upset that maybe this type of approach and by calling people "terrorists" actually drove even more citizens away from the objective that was insistently wished for, and that is vaccination (so, the primal objective was vaccination and not a united society or going through the crisis together and getting out of the crisis even stronger as a society than before).

But we believe that the biggest problem with the narrative above was not that an elementary public communication mistake was made and many citizens were insulted from the highest level as being "terrorists", but the biggest problem is that somebody actually could conceive of such a thing. The problem is that someone, advisors of this public person or maybe even the public person himself actually thought that these citizens would resemble terrorists or, maybe even worse, would wish to discredit them by associating them to terrorism. And if someone responsible for communication thinks like that (and they are not an isolated incident or individual), we should consider that person may be under the influence of a bias. **This is exactly why we consider that the true problem of current strategic and public communication is actually a sociological one**, because this is how people think in certain entourages.

Thus, the sender of public discourse does not care about or does not manage to understand his or her recipient anymore, but they are actually trying to model the recipient according to their own ideological ideas. But what happens to the ones that cannot be modeled? Do we insult them as "terrorists"? The different ways in which such an imagined scenario could go are nothing to be proud of for any human society, especially for a society that thinks of itself, in many aspects, as the best there ever was, up until now.

Basically, this strategic communication mentioned above does nothing but to contradict its own main principles cited at the beginning of the analysis: instead of having cohesion and building trust in society as primary goals, we have a different purpose here, and that is vaccination, wrongly considered a priori as identical to or more important than cohesion and trust. And when we see that this objective of strategic communication that was wrongly taken on is not being adopted by a large segment in the population, what do we do? Instead of making good on our retreat, instead of retreating to new common ground, instead of trying to achieve cohesion and build trust on new factors, do we want to push away and to ostracize an important part of our society that does not do what we want them to do? Then there is no wonder that we seem to have emerged from the pandemic crisis even more polarized and disunited than before.

We wonder how is it that some societies get over crisis and seem to become more united instead of giving way to fractures. They may be doing so because the main objectives of their strategic communication are centered on creating cohesion and building trust in their society no matter what happens on a certain issue, and not by trying to impose a certain issue on the society at the expense of unity and trust. So, things do not go the other way around. And then we could ask ourselves again, why was the strategic communication handled in such a bad way? Because of the same reasons of sociological and ideological bias mentioned earlier.

We can find more famous examples of narratives at Balau M. (2020) and on HotNews (2021) – even though there are also other issues beside the Covid pandemic when a segment of the population was treated with some disrespect by some public communicators, thus missing out on the most important thing – we are all here together and it is only together that we will be able to build a better life and a better society –, when in different circumstances people made public analogies between functional analphabetism and vaccination rates, that is they compared the decision to vaccinate or not to being a functional analphabet. It is hard to conceive not only that these kinds of statements were part of a public or strategic communication campaign, but that these ideas have even been thought in the first place.

Which brings us again to the real problem mentioned earlier, and that is a sociological one – where the sender of communication does not understand or does not want to understand the recipient, a large segment of the population that the sender represents, and, moreover, even treats it with disrespect, superiority, a certain amount of despise as well. And people feel these things and they only antagonize citizens even more. Which is the exact opposite of what a public communication campaign should do or mean for a society.

As an example of communication that would have united a society (or at least would have made no new fractures), in the context of that really difficult pandemic crisis, it could have been said that:

> *"We, the Romanian State and Government, have purchased enough vaccine shots for everyone who wants to get vaccinated, we have managed to equip the hospitals to the best of our capabilities in this*

very difficult moment worldwide, we are doing the best we can to have enough medical personnel, medical equipments and medical supplies. However, citizens should understand that intensive care beds are limited, and so are some medical treatments, it is possible that these may soon become scarce or unavailable if the number of severely ill patients increases, which could mean less appropriate medical care for some and more victims.

Having said that, We, the Romanian State and Government, strongly recommend vaccination. However, we will not instate mandatory vaccination, the Romanian State understands and respects different opinions in the society, understands that vaccination is a personal matter for each citizen, that it requires self-conscious choices, weighing the information that we presented above.

In these circumstances, it is the responsibility for each of us to do as they think is best. The responsibility of the Romanian State and Government is to adequately inform the citizens and to do our best to provide them with medical care, equipment and supplies, with vaccine shots for each citizen that chooses to get vaccinated, in these very difficult circumstances for the whole world, and this is exactly what we have done and will continue doing." (Author's suggestion)

That is all. And it would have been a very professional narrative that would have managed to do exactly what the theory at the beginning of the analysis said it should do: that is informing people and social cohesion, inclusive for the entire society. Not to mention that it may have actually convinced even more people to get vaccinated than the actual narrative that deemed people as "terrorists" or "functional analphabets". It would have been a common-sense message that each and every citizen could have related to.

And this is what it is all about – that all citizens can relate to our message, because we are interested in the unity of the society, cohesion before all, inclusion and the realization that we need to go together ahead with our society even if we do not agree on all the issues with each other, even if we lose sometimes and things will not be perfect, but we win by being united. Because we really need each other, don't we?

Sociological Perspective

The Problem. Ideological Bias. Confirmation Bias. The things mentioned earlier about the Covid pandemic were just examples. Because nowadays, whether we like it or not, public communication has managed to become a means of ideological dissemination on a number of issues. Public communication is no longer about unity, it is not interested in the unity of the society, it is about building arguments or excuses for certain actions and policies ideologically motivated and issued, which means it is about the fourth effect acknowledged by Bernard Miège at the beginning of our analysis as being charged with negative implications. It is about rebuilding a society. And as long as we fool ourselves that we are "only" trying to communicate and to inform just so "we can be educated", but at the same time we are very well determined beforehand about what is right and what is wrong, as long as we think about ourselves as being faultless, then we are under the influence of an ideological bias.

Because, in order to give examples as well, how could we otherwise interpret the fact that there were (rightfully) written lots of analysis on the fake news and disinformation that ran through a part of our society during the Covid pandemic, but there was no analysis written by us, who talk all the time about fake news and manipulation and disinformation, about what was at that moment the unequalled campaign of fake news, disinformation, manipulation that came from the other part of our society in 2018 and tried to convince people to boycott the Referendum to define *the family* in the Constitution (and succeeded in doing so)? How did we miss that huge disinformation campaign? There was evidence for analysis on a level almost the same as the pandemic one in quantity and probably even more in violence than the pandemic one, especially online. Why did we not do any analysis? It is simple – the same ideological, sociological bias, that is hurting all of us so much.

And there is also a confirmation bias here, the way we find it defined by Martha Whitesmith in "Cognitive Bias in Intelligence Analysis: Testing the Analysis of Competing Hypotheses Method": "Confirmation bias is the tendency to search for evidence that supports a preconceived or favoured theory, to interpret information to confirm a preconceived

or favoured theory, or to ignore or unfairly discredit information that would disprove a preconceived or favoured theory." (Whitesmith, 2020, p. 184). Which is exactly what a part of our society did.

Trust. As we showed in the beginning of our analysis, when we talked about the objectives of strategic communication, if we want to have an even better and more functional society, we need to have a united society, based on truth and trust, impartial. If we think we can regain the trust of our society in any other ways, we are mistaken. And we should not even think about gaining trust in other ways, because truth, impartiality and strengthening the social bonds are, in theory, an inherent condition to the public institutions in a society. And, as we well know it and numerous analysis show, the trust of the society is a big problem to which we have thoroughly contributed ourselves, in the academic world – while, as a paradox, we think we are doing the right thing, that we are somehow new "apostles" of an ideology, of democracy and inclusion and "tollerance" and no one else can teach us anything more about these, we forget or leave aside the exact basic instruments that help build trust in society and all the other advantages that come from it. And the moment we thought the above, we have lost the right to be true ambassadors of the values listed there.

It is the same regarding fake news – we are all aghast and upset that a lot of citizens fall to fake news, while at the same time we do not want or we cannot realize why this is happening – because of a critical lack of trust in state institutions (LARICS, ISPRI, 2022), lack of trust based exclusively on the fault of their representatives, lack of trust that can not always be solved by communication – it needs facts, action as well. So, we, as senders of messages, if we believe or expect that we can fix it all just with words, then we are mistaken and all we do in that situation is add more fuel to the lack of trust by exactly the things we are saying – that is by saying and pretending we can fix just by words things that everyone knows should be solved by actions as well.

And if we do not communicate the truth, how can we stand up to the lies? By another lie? Maybe some people would say that works, that it all depends on how efficient and professional the communication is – a maybe it works but only for a while, and the side effects are horrible –

and this is exactly what happened to the Romanian society after decades of "communication" instead of action as well. **Communication that disregards facts or truth lacks consistency and all it does is that it manages to discredit itself in time**.

We believe that it matters a lot to what end do we communicate – if our communication starts from the idea that all we want to do is make the target group believe or do something that we want them to do (no matter if we believe that *something* to be true or not), then we open the path for conflicts in the society on the medium and long-term no matter how professional our message is, because we actually do not care about our target group or we hold it in disregard. Communication becomes a monologue; it does not go both ways anymore. And we all know too well that often the "civil society" we hold so dear and we like to talk with does not represent everyone, that there often is a silent majority, and the "civil society" is often just an excuse to justify certain policies, especially when we like a "civil society", but we do not like another; so, bias again.

If, on the other hand, our communication starts from the idea that we want to create harmony in a society, that we want to create solidarity, trust and consensus by non-coercion for common good (which we may not even know ourselves beforehand which is that), then inevitably we bend down to listen and understand this society in spite of our new or old ideological perspectives, in spite of biases or prejudice and in a very humane way we realize that we are actually part of this society as well. Communication coming from outside of a society has on the short or medium-term less chances to succeed than communication coming from the inside, which is exactly where we should think of ourselves as being from as well. Actually, Pierre Zémor, cited at the beginning of the article as well, argues that two of the main functions of public communication are "to listen (the expectations, questions and public debate), to contribute to ensuring social networking (the feeling of collective belonging, taking into account the citizen as an actor)" (Zémor, 2003, p. 27). We should ask ourselves whether we are doing that.

Superiority complex. The paradox is that we are or we are capable of being truly objective and relevant only if we truly care as well, because otherwise we cannot understand the realities and needs of the target group. And regarding the needs and realities of a society like that

of a nation-state like Romania, realistically speaking, if we think of ourselves as being above it, on the side of it or outside it instead of being part of it, then our communication will not reach the real problems of this society and risks being compromised. Just as it has been compromised, unfortunately, to a different degree, almost every message in the Romanian society because of a lack of trust. Lack of trust generated, as well, by a superiority complex resulting from the public communication of some representatives and some policies, both in Romania, and in the rest of Europe, in general. And this lack of trust has a deep impact on general security too, as we will show below.

Impact on Security. Perspective

Afghanistan. It was already in 2010 that, in the context of another crisis, *NPR* and *Foreign Policy* published an article where there was issued a warning about the American and European superiority complex: "In simple terms, we can now see that the United States and much of Europe were like happy drunks enjoying a pleasant if prolonged pub-crawl. But eventually the party has to end, sobriety returns, and the hangover must be faced. (...) If this analysis is even partly correct, then we are going to need some serious rethinking of grand strategy in both Europe and the United States. Hard choices will have to be made, and traditional world-views and familiar platitudes won't help us very much. Experience is a valuable trait for policymakers in normal times, but it can also blind them when new circumstances arise and the conventional wisdom is no longer relevant." (Walt, 2010) And what do we do in this difficult context nowadays? Do we go forward with our ideological biases that cleavage our society?

And if we want to know where this superiority complex might take us, all we have to do is take a look at many analyses that identified this moral superiority complex as being responsible (among other things, sure) for the painful American disaster in Afghanistan. We cite from an article published in *The Washington Post:* "U.S. leaders must rid themselves of a crusading impulse and a moral superiority complex in international affairs that has done more harm than good to the nation.

Instead, they should recognize the limits of hard power and show humility, prudence and respect for other cultures." (Gerges, 2021)

Everything that was stated above seem remarkably similar to the phenomenon that we are analyzing here regarding European and Romanian politics and communication – which is a moral superiority complex that neither admits, nor tries to understand others and causes a lack of public trust. We surely do not want a societal disaster in the European or Romanian society similar to the American military disaster in Afghanistan and yet we make the exact same mistakes The United States made in Afghanistan and we insist on making them. Considering all the gravity of this potential situation, but both the United States and us should regard what happened in Afghanistan (which came after a semi-failure in the Middle East and Irak) as a warning – if we do not change our approach, if we do not get over this moral superiority complex (which should not be, however, thoroughly mistaken for exceptionalism), just as the analysis cited earlier warned us, then, at one point, "hard power", military or political or even economical power, might not be enough, with catastrophical consequences for both Romania and the entire Western world. And we definitely want to avoid that. This is exactly why, in the context of the rise of China, of the competition, rivalry or emerging confrontation with China, the Russian Federation or other important international actors, like Iran, for example, and others, we must not take things lightly and we must learn from our mistakes. Both from our military mistakes, and, maybe, especially, from our societal mistakes, that have long lasting effects, harder to indentify and potentially more dangerous.

We need to keep our societies united, especially as we notice how adverse societies tend to get together into rather united blocks, both political, economical and in the respect of the general attitude towards the Western world. It may be easy for us to forget this or, sometimes blinded by conventional learning, just like the text cited earlier mentioned, it may be easy to miss the huge global changes that are occurring all over the world, in so many ways.

If we keep doing things the way we are doing them right now, we risk alienating not just places like Afghanistan, but important segments in our own societies. Do we really want to do that no matter the cost? We

can easily imagine how hostile entities like the Russian Federation (which is not at all alone in this regard) can and will not miss out on such opportunities, just like they showed. Especially as, while they profit from this, we do not want to admit the real reasons behind our ever more fractured societies, we exclusively blame the Russian Federation (which is really ok for them, because in our doing this they know we are failing to address the real reasons) and we persist in making those mistakes. Maybe our current narratives, under the influence of sociological biases and a moral superiority complex, exhonerate us from any blame, but the future problems will not be hampered by these at all.

The Communication Problem – A Sociological Problem. Just as we stated earlier, current communication problems are, in our view, actual sociological problems. And it is obvious that the senders are to blame for most of the problems. Because we have to assume that the sender communicates to a receiver they understand. That is part of the job of the sender, to understand and represent the receiver. And if you do not actually understand the receiver, if you just think you maybe understand them, but instead you are under the influence of stereotypes, prejudice, old or new ideologies, then it is obvious that, as the sender of messages, you are the problem. Even though it is difficult for us to admit it, we have to seriously consider this.

Public Communication to a Nation. We have to find common ground, but we have to do this in a very responsible and people-orientated way, because we all know how important communication is, how it can save a society or how it can be used as a weapon against it. And we also have to be aware that when we use this tool for personal, group or ideological purposes, then we are making problems in a society much worse by compromising maybe the only tool that can unite, consolidate our society today, especially in the digital era – and that tool is public and strategic communication.

And we can easily notice this when we take a look at both: communication used as a weapon by old or new authoritarian regimes, and at communication used to save and consolidate a society, like in the case of Ukraine, nowadays. Because the President of Ukraine, Volodimir Zelenski, did not run at the beginning of the invasion, he did not leave the

capital, he felt and acted as part of the society, he took a risk just like the other members of the society and his message was real and concerned the exact real problems his society was facing. He could understand his society when he felt its exact problems, when he was part of it, and, thus, he could speak "its language". Because in the end this is what it is all about – **in order to be able to communicate to and reach a society we have to know and speak its language – not in a linguistic way, but in a societal way.** How could we efficiently communicate to a nation during a crisis (and crisis are one after the other nowadays) if we regard ourselves as being outside that nation or if we somehow disconsider a small or large segment of it or if we believe we know beforehand all of its problems, without even listening or understanding it?

Distrust. Marginalization. The Ideology. And all of these things can easily be felt by part of the society which, later on, often because of distrust, falls victim to disinformation and fake news. And afterwards, of course, it is so easy to point fingers and say that they are "uninformed", "uneducated", "conspiracists", "anti-democrats" and "pro-Russian", "functional analphabets" or "terrorists" etc., but we really have to ask ourselves whether we really did everything we could, whether communication coming from the European Union or from us, all the others, really did everything it could so that these people sat right beside us? Or did we actually drive them away with our elitist communication, ideologically biased communication or just plainly ignored certain serious social problems and focused instead on non-essential issues, solely ideologically justifiable? Didn't, we do all of that?

Discrediting. It is indeed really easy to discredit part of the society after you may have neglected its concerns in your policies or public communication campaigns, its needs, after maybe you let it fall victim to disinformation, maybe sometimes even on purpose, in order to discredit it or its ideas, because you do not agree to its ideas. Maybe just because decidents or the senders of public messages consider a priori that these concerns or needs are illegitimate or obsolete, coming from "The Middle Ages", as unfortunately some people sometimes refer to them in our society as well. And is this how you unite a society or this is

how you want to actually get rid of part of the society? It sometimes seems and feels like a communication lynching.

Not everyone resisting some policies of the European Union are implicitely pro-Russian and not everyone supporting these certain policies in Bruxelles stay far away from doing profitable business with the Russian Federation at the expense of our security (former German Chancellors Gerhard Schröder and Angela Merkel are perfect examples). And then what do we do with this part of the society that is not pro-Russian, but just happens to disagree with us on some internal policies? Do we estrange it, do we push it into the hands of Moscow because of our ideologies, just like we have been doing for the past 10-15 years? And in the meantime, the representatives of this part of the society have conducted very profitable business with Moscow and increased Moscow's leverage on European security for a number of reasons. So, we are offering Moscow (and not only Moscow, but to any other adversary) a double win – while we alienate our own societies? And yet we have been doing all of that for the past 10-15 years.

And even though now it may seem that we have a good chance to rebuild, with great cost and effort, a certain security in regard to the Russian Federation, societal problems, fake news, disinformation campaigns, alienation and radicalization of the society (both left wing and right wing) will only get worse if we do not realize on time what we are doing wrong.

Example. In order to give an example, as a paradox, the Russian Federation does not have at all a lot of popularity in Romania out of several historical reasons, but at the same time there is also a certain distance in the Romanian society regarding certain policies of the government in relation to Ukraine. (Krastev & Leonard, 2022) We ask ourselves why is that? It is definitely not a pro-Russian attitude, then what is it? Apart from certain historical factors, again, one of the answers is the systemic lack of trust in state institutions (LARICS, ISPRI, 2022) – when these state institutions get really focused on certain policies, then the first impulse of the society is to say no, to go the other way. And this is a direct consequence of different policies and statements and communication campaigns during the pandemic and years before that,

which have eroded trust and did not represent the people, did not speak their voice. This is just an example of how this fracture in society can have a serious impact on security.

And there will be more crisis, more circumstances that require very serious security concerns and we just cannot afford to have an alienated part of our society just because some of us systematically drove it away with ideologically generated policies.

We really have to be aware that the distance between two parts of our society is increasing from one crisis to another, instead of decreasing, and if we go on with these ideological biases then we will generate a number of radical attitudes, both on the left, and on the right, all over the European continent, not only in Romania.

Plea for a United Society. We are living in difficult times, complicated and challenging, both internally, and externally, and as long as some of us may believe that they can get through it all on their own, without being part of our society, without *the others*, no matter whom these *others* are, and then we are mistaken. Because we will end up even more fragmented and vulnerable than before.

We have to go back to the beginning – a strong society is, above all, a united society and not an ideologically uniformized society, not matter if it is on the left or on the right. The concept of unity and the concept ideological uniformity are two very different things. Actually, this is exactly what the European Union motto "United in Diversity" wants to say, even though, unfortunately, too often people in Romania or throughout Europe forget its true meaning.

Conclusions

The Initial Purpose of Communication. When there is a fake commited, when one of the primordial meanings of communication is distorted, this is the purpose to generate solidarity and common ground to the benefit of all the members of the group, then society can feel it. Even though most members of the society cannot verbalize it like that, they do feel it and trust is lost – which is exactly one of the biggest problems of our society. Do we want to regain trust? If we do, then public

communication has to be true and not fake, it has to follow in its original objectives and has to be about the real problems, and not about ideologically motivated concerns that only interest a part of it (often the less numerous parts of it). We all know situations when things were and are like that.

Public Communication vs. Political and Ideological Communication. It is often stated in academic literature that public communication should be different from political communication (even though many people mistake one for the other), but it is just as well that public communication should be differentiated from ideological communication, should be protected from being turned into an instrument of ideological propaganda. We are saying this again; the receiver can feel these things and then both communication in general and the public institution are subsequently compromised when we do that. With a very serious impact on the whole of the society and on the security of everyone, that keeps adding to previous problems and impacts.

To make a difference between the two that is between public communication and propaganda let us take a look at how Le Nef defined them (apud Baylon & Mignot, apud Stănciugelu et al., 2014, p. 338):

- "**Public communication** is an impartial sender which is not vassal to any particular entity, may it be a power, group or person."
- **What is propaganda?**

"- It disseminates belief in its primordial meaning, fights so that public opinion accepts certain political or social opinions, and supports a political view, a government, a representative;

- It is a set of information tools that are deliberately used in service of a theory, a political party or an individual, so as to gain support and endorsement of as many people as possible;

- It serves any political strategy as long as it is exploited favourably by scientifically elaborated means of convincing spirits".

We believe that these are quite explicit in revealing what this analysis is also trying to say: **out of sociological reasons, we have diverted from the public communication of a neutral sender**

towards ideological communication, towards ideological propaganda, many times not even realizing it ourselves, and the state of our society is a direct result of these actions. Nowadays, every time we talk about disinformation, its success, how to fight it, when we talk about failed public or strategic communication campaigns (even though we do not talk about that so much, probably thinking that if we do not talk about them, that might save face), **it seems that we are trying to address the consequences instead of what caused them in the first place**, and the Russian Federation is not at all the only causeout there.

All of the above are an insight into one of these causes, a „root cause"**,** as we see it, inflicting both societal, and security and even geopolitical damages, as we showed earlier. Of course, it would be easy to dismiss it, not to admit it for what it is, and this is exactly the reason why it is so widespread and will, unfortunately, continue to be for quite some time. This is the reason why its impact and proliferation are at such a wide scale.

Maybe some people would cinically, ideologically think that this is an impact we can afford, a sort of "collateral damage" for "the greater good", but when we are talking about the future of an entire society, that would be a very dangerous way of thinking and not at all a path we should go on. Especially as we would be doing that while at the same time pretending to do the opposite, which, again, people feel and drives the population even more apart from essential public institutions.

We have to seriously consider all of these things and we have to be honest with ourselves about where we are and what we want to do – do we regard public communication as a tool to change ideological or political views of a target group, no matter what, or do we see public communication for what it was meant to be from the beginning, that is a means of information and of consolidating, uniting a society for the common good? We believe the best idea would be to turn back to its original objectives, that is to inform and to increase social bonds, otherwise we risk emptying and discrediting one if not the most important element of a functional society, with negative consequences which, among disinformation campaigns, conspiracy theories and lack of

trust in public institutions and authority, may still be only at the beginning.

References:

1. Alexandru, M. (2021). *„Campania de vaccinare trebuie să continue cu toate tipurile de vaccin".* G4Media. Available on https://www.g4media.ro/ (accessed on 30.06.2022).

2. Balau, M. (2020). *De ce refuză românii vaccinul anti-Covid. Psihiatrul Gabriel Diaconu: Foarte mulți sunt analfabeți funcțional în ceea ce privește educația medicală.* PS News. Available on https://psnews.ro/de-ce-refuza-romanii-vaccinul-anti-covid-psihiatrul-gabriel-diaconu-foarte-multi-sunt-analfabeti-functional-in-ceea-ce-priveste-educatia-medicala-459669/ (accessed on 30.06.2022).

3. Cornish, P., Lindley-French, J., Yorke, C. (2011). *Strategic Communications and National Strategy, A Chatham House Report.* Available on https://www.chathamhouse.org/sites/default/files/r0911stratcomms.pdf (accessed on 29.06.2022).

4. Gerges, F.A. (2021). *The U.S. squandered the world's sympathy by invading Afghanistan and Iraq. What will it learn from defeat?* The Washington Post. Available on https://www.washingtonpost.com/opinions/2021/08/19/us-afghanistan-invasion-9-11-attacks-lessons-defeat/ (accessed on 30.06.2022).

5. HotNews. (2021). Available on https://www.google.com/amp/s/www.hotnews.ro/stiri-politic-25069944 (accessed on 30.06.2022).

6. Krastev, I. şi Leonard, M. (2022). *Peace versus Justice: The coming European split over the war in Ukraine – ECFR/452,* European Council on Foreign Relations. Available on https://ecfr.eu/wp-content/uploads/2022/06/peace-versus-justice-the-coming-european-split-over-the-war-in-ukraine.pdf (accessed on 30.06.2022).

7. LARICS and ISPRI (Informational Warfare and Strategic Communication Laboratory and „I.C. Brătianu" Political Sciences and International Relations Institute of the Romanian Academy). (2022). *Barometrul de Securitate a României, November 2022 Edition.* Available on https://larics.ro/wp-content/uploads/2022/11/Barometru-de-securitate-a-Romaniei.pdf (accessed on 29.11.2022).

8. Mârzac, E. (2019). *Comunicarea Strategică în sectorul de securitate şi apărare. Notă Analitică, nr. 4*. Available on https://ipre.md/wp-content/uploads/2019/06/natao-pb-nato-marzac-final.pdf (accessed on 29.06.2022).

9. Miège, B. (2000). *Societatea cucerită de comunicare*. Iaşi: Polirom.

10. Stănciugelu, I., Tudor, R., Tran, A., Tran, V. (2014). *Teoria comunicării*. Bucureşti: Tritonic.

11. Walt, S.M. (2010). Article published in *NPR* under the title *Foreign Policy: America's Superiority Complex* and in *Foreign Policy* under the title *The end of the world as we know it?* Available on https://www.npr.org/templates/story/story.php?storyId=126827639 and on https://foreignpolicy.com/2010/05/13/the-end-of-the-world-as-we-know-it/ (accessed on 30.06.2022).

12. Whitesmith, M. (2020). *Predicting Confirmation Bias. In Cognitive Bias in Intelligence Analysis: Testing the Analysis of Competing Hypotheses Method (pp. 184–206).* Edinburgh University Press. Available on http://www.jstor.org/stable/10.3366/j.ctv182jrtn.10 (accessed on 30.06.2022).

13. Zémor, P. (2003). *Comunicarea publică*. Iaşi: Institutul European.

CROSS-TRAINING AS A MODERN PHYSICAL TRAINING METHOD USED IN THE MILITARY FIELD

Gabriel CRACANĂ[*]
Tudor VIRGIL[*]

Motto: "*The lack of activity destroys the good condition of every human being, while movement and methodical physical exercise saves it and preserve it.*"
Plato

Abstract:

In regard to public and strategic modern communication, at least in one respect Considering the armed conflicts near the border of our country, more attention should be paid to national security; thus, all public institutions responsible for national security and defence should focus more on the combat training of subordinate personnel. As a NATO member state and through the role that our country has within the Alliance, in order to prove that we are a strong and respected state, we must constantly make efforts to be able to rise to the level of our partners within the Alliance. In this sense it is necessary to make progress regarding the use of the latest information and communication technologies, the modernization of military techniques and equipment, but also regarding the improvement of the level of physical training. In order to improve the fighting ability of the military, it is necessary to increase the level of their physical training, which can be achieved in the shortest possible time based on the methods and means of training used by the modern armed forces and their implementation in the design of physical training programmes from the very beginning of the military career.

Keywords: *national security, defence, military physical education, cross-training, physical training.*

[*]PhD student at the National University of Physical Education and Sports, Bucharest, email: gabrielcracana@yahoo.com
[*] Professor PhD, National University of Physical Education and Sports, Bucharest, email: virgiltro@yahoo.com

Introduction

Physical education and sports are currently a means through which nations affirm their physical and mental potential as well as their educational, organisational and economic efficiency. The current concept of physical education represents a stage in the evolution of the notion. Initially the notion of gymnastics was used, which now has a narrower meaning that includes its well-circumscribed branches. The transition to the concept of physical education was due to the broadening of the scope of this latter activity, the diversification of its content and forms of organisation, as well as the growth of the population segment engaged in its practice.

In Romania, the concept of physical education is expressed by the *Law on Physical Education and Sports* (2000) as follows: "Physical education and sports are the activities of national interest supported by the state. In the sense of this law, physical education and sports are understood as all forms of physical activity that are intended, through organised or independent participation, to express or improve physical fitness and spiritual comfort, to establish civilised social relations and lead to achievements in competitions of any level."

Physical education is one of the important components of education, influencing individuals on several levels, such as: motor, intellectual, affective, aesthetic. According to Cârstea (2000, p. 26), "the essence of physical education and sports consists in the fact that the practice of physical exercise, regardless of the organisational form and the socioeconomic or political formation in which it is performed, mainly aims to improve the physical development and motor ability of the participants."

Physical training is an indispensable component in the training process for all personnel in institutions with attributions in the field of national security and defence and has an important role both in terms of optimizing the capacity for combat and in their continuous professional training. Physical training should be a priority in the military field as an optimal level of physical training of the military directly contributes to the increase of efficiency and specific attributions for the fulfilment of various missions, even in difficult situations.

The purpose of this paper is to highlight a modern approach in the process of physical training of military personnel by introducing and using the newest training methods that contribute quickly and effectively to increase the physical potential of the military. Thus, *cross-training* means both a philosophy of movement and a competition with oneself, incorporating intense workouts that involve aerobic and anaerobic exercises, weight training exercises, elements of isometry, combinations of gymnastics and athletic exercises, bodyweight exercises. By implementing this training method in physical education lessons specific to military higher education institutions, the future military personnel will be able to go beyond their ordinary limits and improve their fighting ability.

The current situation of military physical education

People are a very important factor in the evolution and existence of a society and, in accordance with social requirements, they constantly seek to improve their psyche, intellect and physical potential. The great military powers, insisting on the need for combat training, actually highlight the need for multidisciplinary training, including elements of military tactical training, topography, engineering, telecommunications, shooting with different categories of weapons, first aid, all of these achieved on a very good foundation of the fighter's body which should be equipped with a very strong mental and emotional side. This reveals the role and importance of the human physique in the success of a mission.

Military physical education, as a component of general physical education, was created by adapting physical education to both the combat training needs of military personnel and the specifics of their missions.

Military physical education is organized and carried out in all units, subunits and military educational institutions, according to specific training plans and programs, their content being determined by the general requirements of the training process, by the specifics of each weapon and military specialty.

The lack of research and the unscientific way of approaching physical training in the military field has led to monotony and low student motivation because the traditional means and methods of

training are often outdated. According to the *Military Physical Education Regulation* (2012), the military physical education lesson represents the main organisational and functional unit of the training process. It is carried out on the basis of specialised programmes under the guidance of an expert and with the mandatory participation of all established personnel. The training process in military institutions includes multiple didactic activities aimed at optimising motor and learning skills, consolidating and enhancing utilitarian-applicative and sports motor skills, but also actions focused on educating body posture and even correcting some physical defects, which is why this specialty is fundamental for training the qualities of a fighter.

Physical education in the military field is a basic form of long-term education, which should lead to a healthy lifestyle, a way of thinking and acting for both one's own benefit and for the social interest. Starting from this idea, we could change the mentality about the content and especially the management and organisation of physical education in our country.

The process of switching from exclusively biological influences to multilateral, educational, psychological and social ones involves, on the one hand, using physical education as a form of general education, and on the other hand, forming an individual's conviction to practise physical exercise in all stages of life. The modern military environment requires developmental changes in all its areas of interest, starting with the theory of military art, the management of military actions, the technological upgrading of armament and combat techniques, and ending with training at the individual level.

In recent years, attempts have been made to revive the field of physical education in military institutions through the objective way in which it has been viewed by the leadership factors in the army as well as due to NATO membership. Participation in international missions alongside allies is a good opportunity to observe how this category of training is regarded by modern armies, and the role and importance of the specialist in the field has been emphasised by both the application of the designed physical training programmes and the high exercise capacity of the targeted individuals.

The objectives of military physical training

Physical training in the Romanian military environment, as a component of combat training, has been addressed over time without exhausting all its resources; instead, opportunities have been created to update the information and develop other new directions of analysis. According to the armed forces of NATO member countries, physical training aims at the general physical development of the military and increasing their specific exercise capacity. This enhances their efficiency and permanent state of mental alertness, promotes cohesion and raises the level of maintenance and development of combat capability, thus contributing to the formation of a well-trained military man able to withstand tension and stress. Certainly, very good physical training will result in maximising the moral-volitional and physical components of the fighting ability and will help to strengthen overall physical health, developing resistance to states of stress such as fatigue, fear, panic, hunger.

Being the starting point of the entire physical training process for the military and a subsystem of physical education and sports, military physical education is a component of the training process that exploits all forms of collective or individual activity carried out in order to build, develop and maintain motor skills necessary in situations of peace, crisis and war, thus contributing to the improvement of the physical and mental health of military personnel (*Military Physical Education Regulation*, 2012). Such personnel should be prepared for an ever-changing society characterised by dynamism which requires a certain intellectual, moral, physical and civic configuration, a certain profile that harmoniously combines the sides of each individual's personality: a healthy, harmoniously developed and highly-skilled military with creativity and fast thinking skills, initiative, the ability to select, systematise and reorganise information, to choose the best solutions and quickly decide on their application in practice.

Physical training is a very important component in the military career, which directly contributes to the training process of the military and positively influences their ability to perform, at an optimal level, in emergency situations encountered both in their professional activity and in everyday life.

New trends in the physical training process of the military

Cross-training is the most modern training method that is commonly used in the physical training process by the defence system structures at the international level; this method is used by the military, firemen and policemen but also in the academic environment, especially in NATO and EU member states. Cross-training means both a philosophy of movement and a competition with oneself, incorporating intense workouts that involve aerobic and anaerobic exercises, weight training exercises, elements of isometry, combinations of gymnastics and athletic exercises, bodyweight exercises.

Updating the relevant literature is a necessary action that underlies any scientific activity. Previous studies on military physical education represent a global whole, but in order to add value to the research, we should not limit ourselves to this horizon but bring our own contribution to the physical training of military personnel. In recent years, due to the participation in joint missions with the other NATO member states, military physical training has significantly developed because the military observed and adopted the way of approaching this indispensable component for their field of activity.

Proper physical training provides the physical and mental support needed by the other categories of training; therefore, we should highlight the importance of the specialist who, through the designed programmes applied in the training process, represents an essential element in the training and education of the military. Considering both the practical and applied nature of military physical education, it ranks among the disciplines with great possibilities for achieving the general objectives of the military field. In this regard, it contributes to increasing work capacity, providing the military with transferable abilities, skills and habits in productive activity, developing motor skills required in these activities and getting used to team spirit, group activities, discipline, order and exigency.

Although the object of the activity is the person knowledgeable in the field to follow, besides the part of knowledge and research, it is necessary not to neglect the formation of moral, aesthetic and physical qualities, which are related to what we call a multilaterally-developed cultural being. As Vințanu (2001, pp. 25-40) highlights: "An emphasis

placed exclusively on the cognitive function limits the research, not taking into account aspects related to sensitivity (such as aesthetic, rational and affective ones), in other words, everything that characterises man as a human being. When the focus is only on changing certain aspects, an imbalance occurs that leads to failure to achieve the general objectives of education."

For their training and development, the military should aspire to improvement from a physical, intellectual and moral point of view in order to become useful to society, and therefore they should always be concerned about their state of health, as well as their ability to cope with professional and daily life demands, and for this, they need to be aware of the importance of practising physical exercise and sports.

The field of military physical education, which is influenced by the development of the instructive-educational process in the military environment, includes numerous didactic activities for learning and improving utilitarian-applicative and sports motor skills and abilities, educating body posture, preventing and combating physical impairments, which is why it represents the essence of the approach to the formation of military qualities.

From a didactic point of view, physical exercise is the main tool in programming and carrying out the training process; therefore, it is a basic component for achieving the objectives of military physical education. According to Șiclovan (as cited in Tudor, 2007, pp. 113-114), physical exercise is "a predominantly bodily action performed systematically and consciously in order to improve the physical development and motor ability of people". The same author claims that physical exercise should be understood as a possibility of permanent adaptation to internal and external conditions and should not be seen only as a stereotyped repetition. In this context, physical exercise does not simply involve systematic repetition but also provides the opportunity to build a form of motor behaviour based on learned movements and assimilated motor knowledge.

In military physical education, general physical training is carried out using means and methods of a general nature or borrowed from other branches of sport with the aim of developing motor ability and increasing the overall functional potential of the body. The content of

military physical training is mainly oriented towards the development of exercise capacity and combined motor skills, which are regarded as priorities. In turn, this training has a general orientation and, in our case, addresses the specificity of each individual profession.

In compliance with exercise physiology regarding the continuous and safe development of exercise capacity required by the increased physical demands on military personnel, the following aspects need to be considered:

- increased efforts throughout the year;
- the predominant use of maximum efforts;
- the use of functional training;
- combining exercise with recovery and rest.

A few decades ago, the American military services concluded that it was necessary to develop new physical training programmes that would stimulate the military to maintain an optimal level of physical fitness to be able to produce professional performance. Nowadays, an ideal training programme should consist of exercises aimed at improving general physical fitness and major body functions.

Cross-training is a revolutionary training method, a reinterpretation of military-type training, which is based on functional exercises, HIIT (High-Intensity Interval Training), calisthenics, exercises involving weight lifting, TRX (Total Body Resistance Exercises), exercises borrowed from different branches of sport (athletics, gymnastics, boxing) and performed with high intensity. Isolated bodybuilding exercises are not used in this type of training. Bodyweight exercises have been used since the time of ancient Greece because they are the basis of any sports discipline and the training of soldiers. Calisthenics represent a whole culture about the training in which bodyweight exercises are used.

Functional training has the main purpose of transferring the effects obtained from exercise into effective daily actions by involving the entire neuromuscular system (Liebenson, 2014, p. 271). This type of training has been adopted by the vast majority of professionals in the field of physical education and sports but also by national security and defence structures that have turned it into a type of training where bodyweight exercises are predominant. The main purpose of functional

training is to improve a person's ability to carry out professional and everyday activities.

High-Intensity Interval Training (HIIT) is a method that mainly uses cardio exercises, which alternate high-intensity with low-intensity exercises. To achieve the proposed objectives, this type of training is much more effective than classic cardio exercises because the exercises performed at the same pace lead the body towards a constant zone, which means that the body adapts to the execution speed and will try hard to conserve its energy. HIIT is a non-conventional and relatively new training method in our country. Another new training method is TRX Suspension Training, which is used by both the military and elite athletes.

Similar studies

Studies in the field of physical education and sports confirm the need to revitalise the instructive-educational process by introducing new means and methods of training. In 2008, Keith C., the director of the Health and Fitness programme at the Globe University of Minnesota, conducted a study where traditional training was compared to functional training. For more than 16 weeks, the researcher trained two groups of adults separately, and the results demonstrated that functional training increased the level of physical training more than in the case of traditional one.

Moreover, in his doctoral thesis entitled *Optimisation of the general and specific physical training of the counter-terrorist intervention group members through the means of physical education and sports* (2009), Paraschiv shows that functional training has an important role in the physical training of counter-terrorist fighters.

In 2018, three USEFS PhD students from the Republic of Moldova conducted a study where they compared the functional training benefits with the traditional training benefits for martial artists. The participants were 40 athletes aged between 18 and 30 years, all martial artists who were divided into two equal groups. The study took place over a 7-week period. The results highlighted that functional training could be an alternative for performance improvement in athletes practising martial arts compared to traditional training. They also indicated that functional

training increased muscle strength, endurance, balance and flexibility (Olaru et al., 2018, pp. 366-374).

It has been proven that a new training method called INSANITY can be successfully used in physical education lessons in military higher education because notable results are obtained in terms of improving the physical fitness of students and avoiding monotony, which is demonstrated in the doctoral thesis *Optimisation of motor and mental skills by modernising the content of the physical education lesson in military education* (Smîdu, 2021).

The cross-training method has started to be more and more popular in our country, having been already adopted and used in the physical training process of competitive athletes and by the personnel working in the defence system structures (policemen, firemen, gendarmes, soldiers). As Boyle (2016) stresses, the implementation of cross-training as the main training method in military physical education brings numerous benefits, such as:

- improvement of the function of the muscular-skeletal system because functional training focuses on the natural movements of the body, without isolating certain muscle groups;
- prevention or reduction of muscle imbalances caused by a vicious attitude;
- body weight control: the use of functional training is an effective alternative to reduce body weight by increasing metabolic rate and decreasing adipose tissue;
- improves strength indices: the body gets a harmonious and vigorous appearance without the muscles being developed in an exaggerated, unesthetic manner;
- balance improvement: this training method includes exercises aimed at enhancing coordination at the intersegmental and intramuscular levels;
- enhancement of the neuromuscular relationship by the integration of functional exercises in the physical training process;
- development of neuromuscular memory faster than in the case of other types of exercises;

- contribution to the formation of an active and healthy lifestyle and to the improvement of all physical fitness components: strength, speed, respiratory and cardiovascular endurance, power, agility, coordination, balance, precision, flexibility, vitality;
- the ability to practise it anywhere (in the gym, outdoors or at home);
- acceleration of metabolism;
- improvement of cardiovascular and pulmonary capacity;
- achievement of an optimal level of physical fitness in a short time.

Conclusions

The regular practice of physical exercise under the guidance of a specialist has an important contribution to shaping self-esteem, maintaining calmness and making effective decisions in crisis situations, develops the capacity for self-control, the power of concentration, and restores emotional and functional balance. The cross-training method is designed for universal application, so it can be successfully used by any person in the national security and defence system, regardless of experience, gender, age or training level.

The implementation of this training method in the field of military physical education provides solutions for increasing the physical and mental potential of military personnel; it is a reinvention of outdated physical training methods that prevents monotony and engages the military in the training process, making them more aware of their role, the importance of physical training and the fact that, as NATO members, we need to rise to the level of the other member states of the alliance, at least from the point of view of combat readiness.

References:

1. Băiţan, G.-F. (December, 2018). "Implementarea noilor standarde privind nivelul de pregătire fizică a candidaţilor pentru profesia militară în SUA." *Buletinul Universităţii Naţionale de Apărare "Carol I",* vol. 5, no. 4, pp. 95-100, available on https://revista.unap.ro/index.php/revista/article/view/802

2. Boyle, Michael. (2016). *New Functional Training for Sports,* Second Edition, Human Kinetics Publisher, North Yorkshire.

1. Cârstea, Gh. (2000). *Teoria şi metodica educaţiei fizice şi sportului*. AN-DA Publishing House, Bucharest.

2. *Legea Educaţiei Fizice şi Sportului*. (2000). Chapter 2, article 7.

3. Liebenson, C. (2014). *Functional training handbook*. LWW.

4. Paraschiv, C. I. (2009). *Optimizarea pregătirii fizice generale şi specifice a componenţilor grupei de intervenţie antiteroristă prin mijloacele educaţiei fizice şi sportului* (doctoral dissertation). UNEFS Bucharest.

5. *Regulamentul educaţiei fizice militare*. (2012). Chapter 1, article 1.

6. Olaru, F., Todiriţa, B., & Toma Urichianu, S. (2018). "Functional training vs. traditional training benefits for martial arts practitioners." *Scientific Bulletin of Naval Academy*, Vol. XXI, pp. 366-374.

7. Smîdu, D. (2021). *Optimizarea capacităţilor motrice şi psihice prin modernizarea conţinutului lecţiei de educaţie fizică din învăţământul militar* (doctoral dissertation), UNEFS Bucharest.

8. Tudor, V. (2019). *Educarea capacităţilor coordinative*. UNEFS Bucharest.

9. Tudor, V. (2000). *Coordonate teoretice şi educaţional-formative, repere pentru elaborarea unui sistem de evaluare la educaţia fizică şcolară* (doctoral dissertation). ANEFS Bucharest.

10. Vinţanu, N. (1998). *Prelegeri despre educaţia sportivă*. Pro Transilvania Publishing House, Bucharest.

PRACTITIONERS' BROAD VIEW

INVULNERABLE – INFORMED ABOUT VULNERABILITIES!

Florin BUŞTIUC*

Abstract:
A hostile intelligence entity is trying to identify or create behavioural vulnerabilities – professional dissatisfaction, unrealistic expectations, gambling, spending/borrowing beyond means, expensive lifestyle, financial difficulties, so as to exploit them to influence the person to reveal confidential information or to adopt certain decisions.

One of the ways of counterintelligence protection of data and decision is the awareness by individuals of vulnerabilities and reality that can be exploited by a hostile entity. And the purpose of a test on vulnerabilities is to evaluate the level of awareness and, implicitly, self -protection.

Keywords: *hostile intelligence entity, vulnerabilities, self-control, non-public/ confidential data.*

Introduction

The aim of this paper is to address the vulnerabilities of a person with access to classified and sensitive information in order to straighten the awareness and *self –protection*. The objective of a hostile intelligence entity[1] is to deliberately obtain certain information about people or organizations (projects, negotiations, research, contracts, etc.) that creates disadvantages for the latter, i.e. it affects their interests.

Frequently, a hostile intelligence entity carries out activities under the cover of a journalist, researcher, businessman, participant in a scientific event, member of a delegation, etc. – thus, the "presence and

* PhD, "Mihai Viteazul" National Intelligence Academy; email: florinnn11@yahoo.com
[1] Some aspects have been taken from the doctoral thesis – *Pregătirea contrainformativă a persoanelor cu acces la informații clasificate/nepublice* – defended in 2021, at the "Mihai Viteazul" National Intelligence Academy.

legitimate activities" of official delegations, private companies, scientific institutes, media organizations, etc.

A hostile intelligence entity builds a relationship with the person of interest, and the existence of vulnerabilities facilitates influencing him to divulge (involuntarily) or engage (voluntarily) in illegal data collection activities.

Vulnerabilities refer to those psycho-social personality characteristics – behaviours, motivations, situations, connections with certain persons / organizations / states – on the basis of which a hostile intelligence entity maximizes his chances of influencing that person. We exemplify the following vulnerabilities:

- **personal difficulties** – divorce, bankruptcy, medical problems, addiction are factors that create the possibility of exerting influence by interested entities;
- **lack of loyalty** – belonging to different organizations of the underworld, the appropriation or use of large sums of money (large-scale financial frauds), the self-interested exploitation of security knowledge to establish possible deficiencies, the provoking and maintenance of a tense atmosphere in the collective, generating suspicion and mistrust among employees, exploiting curiosity and indiscretion or negligence and lack of interest;
- **gossip/boasting** – indiscretions committed through telephone conversations or telegrams or by discussing confidential professional issues in public, in circles of friends or in the family; the imprudence/indifference of officials who describe, with too much luxury of detail, at the various international meetings or specialized publications, the nature of their work, research, discoveries etc.;
- **immoral behaviours or behavioural deviations** that can generate the risk of the person being vulnerable to blackmail or pressure – as a rule, there are "sensitive" situations related to intimate life or things that affect the family climate or social image. In some cases, people are blackmailed by threats to their physical integrity or by exploiting their feelings. Vulnerability to blackmail refers both to the targeted person

and to family or close members, friends, collaborators or other people who enjoy a special condition (children, neighbours, colleagues, etc.);

- **connections with persons who could exert acts of pressure / blackmail**, respectively which could generate exploitable vulnerabilities by hostile foreign intelligence services and organized crime groups;
- **the need for money** – covering expenses related to solving some health problems; payment of debts resulting from gambling, loans from various "friends"; the amazing lifestyle, the satisfaction of personal pride;
- **mental or emotional disorders/alcohol consumption affecting discernment** – equivocal, disorganized behaviour. These people can be used for direct criminal purposes – by subordinating the will – or indirectly, by exploiting the "gray" in their area of responsibility;
- **ideology** – some individuals adhere to certain values/ideas, which, in their view, "are not respected" in the social practices and actions of the institution, and therefore disclose information. (Brown, 2011; NATO Standard, 2016)

In this context, *threats* represent people who directly support the objectives of some entities (intelligence entities or interest groups) to have access to confidential information and create security breaches, and *risks* are acts of collection, transmission, destruction, unauthorized modification of information. In the absence of vulnerabilities, the person resists to influence and refuses involvement in illegal activities. But when there are vulnerabilities, the capacity for resistance decreases, and *the paradox is that in most cases the person does not realize that he/she has a vulnerability or has the illusion that they are in control.*

Being aware of vulnerabilities creates the possibility to give up certain behaviours, to cancel or reduce motivational anchors, to avoid involvement in situations and connections with certain people/ organizations/ states. Consequently, the possibility of diversifying options and professional development is preserved, in the context of an institutional assessment of vulnerabilities in some cases, when access to

non-public data is necessary, and that assessment could result in refusal of access to information.

*

In this context, we appreciate that it is relevant for a person to have the possibility to verify through a questionnaire/test if he is a potential vulnerable person and to address this issue appropriately, and we propose the following questionnaire[2]. There are 27 sentence-statements regarding motivations, behaviours, situations, connections with certain persons/organizations/states, which can constitute vulnerabilities. Determine which is true or false.

1. The feeling of frustration, professional dissatisfaction, feelings of revenge and punishment of the "guilty": the institution/professional management.

□True □False

2. Connections with persons – relatives, friends or business partners – who have residence in a (hostile) state that has been established to be actively involved in gathering information about/from Romania.

□True □False

3. Existence of situations or involvement in activities that could affect public image if disclosed (for example, extramarital affairs).

□True □False

4. The tendency to believe that the interlocutor is in good faith and that he has no hidden interest, a tendency that determines the formulation of detailed answers to questions, even when they are related to professional activity.

□True □False

[2] The instrument is the author's view. Other tools are presented in Florin Buștiuc, (2015). *Minighid de pregătire și protecție contrainformativă – factorul uman & organizația*, Bucharest, Semne Publishing House.

5. Scientific collaboration or consultancy with any person or organization on topics related to professional activity, which has been approved.

□True □False

6. Deliberate omission, concealment or falsification of aspects in biographical statements and official forms.

□True □False

7. Deliberate provision of false or distorted data to an employer or state institutions.

□True □False

8. Connections with a person, group or organization that may create a conflict of interest with regard to the obligation to protect information that is of interest to those entities.

□True □False

9. Fraud, theft from the employer, use of false loan statements.

□True □False

10. Exaggerated optimism, with underestimation of the possibility that one may be a target for information gathering.

□True □False

11. Irresponsible spending and excessive indebtedness.

□True □False

12. Borrowing significant sums to participate in gambling or to pay gambling debts.

□True □False

13. A controlled consumption of alcohol, so that discernment is not impaired.

□True □False

14. Consumption of substances that affect discernment.
□True □False

15. The tendency to propagate negative, exaggerated, tendentious comments about people or situations, which can lead to the disclosure of data about possible dysfunctions in the field of security in the organization.
□True □False

16. Pathological gambling, betting on ever-higher stakes.
□True □False

17. Tendency to discuss work-related matters with family members or friends.
□True □False

18. The cautious attitude and the application of the principle that it is not obligatory to answer all questions, respectively to reveal everything you know in relation to subjects related to professional activity.
□True □False

19. Disregarding or ignoring an organization's information protection rules.
□True □False

20. Participation in various events or magazines with articles or materials related to the professional activity that were previously presented to be approved by the competent factors.
□True □False

21. Talkativeness and boasting that materialize in indiscretions.
□True □False

22. Pride, the tendency to always be right and demonstrate competence.

□True □False

23. The feeling of gratitude, the moral or financial obligations to persons, groups, organizations or states that may create a conflict of interest regarding the obligation to protect information that is of interest to those entities.

□True □False

24. Very high financial needs due to difficult situations – divorce, medical expenses, bankruptcy, etc.

□True □False

25. The belief that we are superior and that the (security) rules don't apply to us because we are different.

□True □False

26. The greed for compliments and sympathy that can lead to the disclosure of some aspects related to the professional activity, in order to recognize the "value, importance, merits" and preserve the relationships.

□True □False

27. Very high lifestyle / standard of living, which cannot be supported by legal income.

□True □False

ANSWERS

The scores are calculated upon the relevance for the vulnerabilities and the sum is 27 points (where false is not in the following table, the score is 0):

1-T-1p	**7- T-0,5p**	**13-F-1p**	**19- T-1p**	**25- T-1p**
2- T-1,5p	**8- T-1,5p**	**14- T-0,5p**	**20-F-1p**	**26- T-0,5p**
3- T-1p	**9- T-0,5p**	**15- T-1,5p**	**21- T-1p**	**27- T-1p**
4- T-1p	**10- T-1p**	**16- T-0,5p**	**22- T-1p**	
5-F-1p	**11- T-0,5p**	**17- T-1p**	**23- T-1,5p**	
6- T-0,5p	**12- T-0,5p**	**18-F-1p**	**24- T-1p**	

How to interpret the scores (the sum of the matching answers points-**p**):

1-9p – Some would characterize you as a "naïve" person, for your opinion that it is not moral for someone to exploit certain negative aspects of the personality. Besides, you don't perceive these aspects as vulnerabilities, but as traits or "events" that need to be accepted by others, and the person counselled to modify them. This option is also possible, but you must be aware that, in relation to professional activity, it is appropriate to interpret reality through the lens of vulnerabilities. A hostile intelligence entity will exploit these traits or "events", and everyone is responsible for being aware of vulnerabilities and developing self-control.

10-18p – As a rule, you identify only "serious" vulnerabilities, such as consumption of prohibited substances, falsification of documents, gambling, significant irrational spending, etc. You are less attentive to the aspects that manifest themselves in the process of inter-human relations and which are subtler, more difficult to accept – to admit that you are a "talker", that you want to be right and impress with professional knowledge, etc.

19-27p – You know very well what the vulnerabilities are, but also the strong points of the personality. You have a very good self-protective attitude, i.e. you anticipate from the beginning that getting involved in certain situations, establishing connections or developing certain behaviours can degenerate into vulnerabilities. You have very good self-control and the ability to manage situations and relationships where information is sought.

Conclusion

Thus, reasonable explanations are invented so that these aspects are no longer perceived as vulnerabilities – you are not a talker, you are a very sociable person who energizes events; you do not disclose matters related to your professional activity, but you are an honest person who presents others with the correct version of a subject, etc. But you have

the ability to accept that your interpretations are wrong and that some aspects of your personality are vulnerabilities.

References:

1. Brown, Andrew. (2011). *The Grey Line: Modern Corporate Espionage and Counter Intelligence,* Kindle Edition, Amur Strategic Research Group, retrieved on June 27, 2022 from https://www.scribd.com/read/206815606/The-Grey-Line-Modern-Corporate-Espionage-and-Counter-Intelligence

2. Buștiuc, Florin. (2015). *Minighid de pregătire și protecție contrainformativă – factorul uman & organizația,* Bucharest, Semne Publishing House.

3. NATO Standard AJP-3.9. *Allied Joint Doctrine for Joint Targeting*. Edition A Version 1. 2016, retrieved on June 30, 2022 from https://www.nato.int/cps/su/ natohq/publications.htm

REVIEWS AND NOTES

Etienne Augris, *Philippe Rondot maître espion. Biographie* (*Philippe Rondot master spy. Biography*), Nouveau Monde Editions, Paris, 2023, 329 p.,

presented by Mihaela TEODOR*

Philippe Rondot master spy. Biography is the title of the book published at the Nouveau Monde Publishing House from Paris, France, in February 2023. The book, signed by the French historian Etienne Augris[1], is the first biography of General Philippe Rondot, a legend of foreign and domestic French intelligence services. The book is considered by experts and reviewers an "unprecedented and rich in detail dive into the career of an essential cog in the wheel of French counterintelligence" or "a form of tribute for the spy Rondot as he was, during his lifetime, an essential cog in the French secret services".

The content is structured as follows: an introductory chapter, *Prologue: Ombre et lumiere* (*Prologue: Shadow and Light*), an *Epilogue: Beyrouth-Chanaud* (*Epilogue: Beirut-Chanaud*) and 12 chapters: *L'héritage familial, de la Lorraine a Beyrouth* (*Family heritage, from Lorraine to Beirut*); *Au nom du père* (*In the name of the Father*); *De 'Ginette' a Saint-Cyr* (*From 'Ginette' to Saint-Cyr*); *L'expérience algérienne* (*The Algerian expérience*); *L'entrée au SDECE* (*Entry to the SDECE*); *Piège a Bucarest pour Rotin* (*Piege in Bucharest for Rotin*); *L'expert e le*

* Senior Researcher in security studies at National Intelligence Academy „Mihai Viteazul"; email: teodor.mihaela@animv.eu

[1] Étienne Augris is a talented professor of history and geography at the Jeanne-d'Arc High School in Nancy, and a regular contributor to the general culture magazine L'Éléphant.

'consultant' (*The expert and the 'consultant'*); *Face au terrorisme et a Abou Nidal* (*Faced with terrorism and Abou Nidal*); *La traque Carlos* (*The Carlos Hunt*); *Libérations d'otage et opérations secrètes* (*Hostage releases and covert operations*); *Missions K et M en ex-Yougoslavie* (*K and M missions in the former Yugoslavia*); *Clearstream, Hubris et Nemesis* (*Clearstream, Hubris and Nemesis*). As a well written scientific research, the book does not miss the *acknowledgements*, the selective bibliography, and the notes.

Philippe Rondot, a French general and a graduate of Saint-Cyr, died in 2017 at the age of 81. Coming from a military family, General Philippe Rondot, was an iconoclastic figure within the French intelligence community, a man of action and also the author of several books: *La Syrie*, Presses Universitaires de France, Paris, 1978; *L'Irak*, Presses Universitaires de France, Paris, 1979; *La Jordanie*, Presses Universitaires de France, Paris, 1980; *Les projets de paix arabo-israéliens*, École des hautes études en sciences sociales, Paris, 1980 (thèse universitaire); *Le Proche-Orient à la recherche de la paix, 1973-1982*, Presses Universitaires de France, Paris, 1982 etc.

The General was involved for five decades in high-profile cases such as the arrest of the terrorist Carlos alias "The Jackal" or the search for war criminals from former Yugoslavia. We can read in the book about the past and the adventure in intelligence of the famous General.

What Romanian readers could be interested in is General Rondot's first mission abroad at his first post as deputy of the French military attaché which was in Romania. He worked there for almost two years (May 1966 - February 1968), being sent by the SDECE (Foreign and Counterintelligence Documentation Service). In the '70s, Philippe Rondot came to the attention of the Romanian Security. In General Rondot's file, which Etienne Augris was able to research at CNSAS, the General had code names as "Rotin", "Radu" and "Racu". In the chapter *Piege in Bucharest for Rotin,* the author of the biography stresses out that it is not very clear

whether or not Rondot fell victim to a compromising operation with a woman. However, he even staged an accident with a car driven by a female driver, not far from Bucharest. More than two decades after his Romanian adventure, in 1992, Philippe Rondot, who had meanwhile become a senior official of the French Internal Secret Services (DST) and coordinator of the military intelligence services, returned to Bucharest. He met with the heads of domestic and foreign Romanian intelligence services, and later he accessed his own Securitate file containing all the spin reports concerning Lieutenant Rondot from 1966-1968.

General Philippe Rondot found himself exposed to the general public in 2004, when the *Clearstream 2* affair[2] broke out and he became "famous". Rondot's famous notebooks, in which the spy diligently noted his smallest actions and gestures since a misadventure which had forced him to leave the action service of the SDECE, published during the investigation were feeding many fantasies and triggered a form of collective madness. However, the justice will eventually recognize his innocence.

The author traces the life of General Philippe Rondot in a well-documented book based on testimonies and original sources. Thus, he acknowledges that the research work took place in various archives and libraries in France such as the Kurdish Institute in Paris, the Historical Service of Defence, the National Archives and Diplomatic Archives, the university libraries of Lorraine and Nancy; and in Romania such as Archive of the National Council for Studying the Archives of the Security. What can be simply said on the book is that it is an excellent biography written by the talented French historian Étienne Augris. The great importance of the book resides in the mysteries of French espionage and counter-espionage of the last century.

[2] See more on Clearstream 2 at https://www.france24.com/en/20090918-how-finance-trial-turned-major-political-scandal-

ACADEMIC FOCUS

Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET)
H2020 Grant agreement no: 883054
(May 2020 – April 2025)

EU-HYBNET is a 60-month project (2020-2025), financed through the Horizon 2020, which start in May 2020. The project is being developed and implemented by a consortium of 25 partners, coordinated by LAUREA University of Applied Sciences from Finland. The European Centre of Excellence for Countering Hybrid Threats and the Joint Research Centre are leading partners of the EU-HYBNET project.

EU-HYBNET bring together practitioners and stakeholders to identify and define their most urgent requirements for countering hybrid threats, by undertaking an in-depth analysis of gaps and needs and prioritizing those that are crucial to address through effective research and innovation initiatives, including arranging training and exercise events to test the most promising innovations (technical and social) which lead to the creation of a roadmap for success and solid recommendations for uptake, industrialization and standardization across the European Union.

The project aims to build an empowered, sustainable network, which:

- define common requirements that can fill knowledge gaps, deal with performance needs, and enhance capabilities of innovation endeavors;
- monitor significant developments in research and innovation;
- deliver recommendations for uptake and industrialization of the most promising innovations that address the needs of

practitioners, and determine associated priorities for standardization;
- establish conditions for enhanced interaction among its members;
- persistently strive to increase its membership and continually build network capacity through knowledge exchange.

EU-HYBNET address four core themes to ensure coherence in the project's results: 1) Future Trends of Hybrid Threats, 2) Cyber and Future Technologies, 3) Resilient Civilians, Local Level and National Administration and 4) Information and Strategic Communication.

Romania represents the consortium through "Mihai Viteazul" National Intelligence Academy (MVNIA). MVNIA incorporate the project's research findings and information into its MA & PhD research programs. As students come from diverse areas (security practitioners, legal, media, private business), the impact of exploitation of the information reach a wide audience, and the EU-HYBNET training documents will also be employed to enhance capabilities of experts and practitioners in the fight against hybrid threats.

EU-HYBNET is a Pan-European network of security practitioners, stakeholders, academia, industry players, and SME actors across EU, collaborating with each other to counter hybrid threats.

With the support of the Erasmus+ Programme of the European Union

Jean Monnet Module
EUSEGOV (2020-2023)
621227-EPP-1-2020-1-RO-EPPJMO-MODULE

Jean Monnet Module EUSEGOV

A common understanding of EU Security Governance
Teaching and researching the EU security policies and institutions for a better academic and professional approach in the security and intelligence field
(October 21st, 2020 – October 20th, 2023)*

"Mihai Viteazul" National Intelligence Academy (MVNIA) implements a three-year Jean Monnet Module grant: **EUSEGOV** – *A common understanding of EU Security Governance. Teaching and researching the EU security policies and institutions for a better academic and professional approach in the security and intelligence field*. The EUSEGOV module focuses on EU Governance, a subfield of EU studies that has received less attention comparatively with the study of other EU related issues. The module aims at educating students and at equipping them with the knowledge and necessary skills to become EU citizens and better security providers. The academic value of the EUSEGOV module is to deliver courses on EU Security Governance for security and intelligence studies students. The courses tackle specific aspects of EU integration studies: *Introduction to EU Security Governance and Strategic communication in EU Security Governance.*

* This Project has been carried out with the support of the Erasmus+ programme of the European Union. The content of this Project does not necessarily reflect the position of the European Union, nor does it involve any responsibility on the part of the European Union.

The **specific objectives** of the Module are:

- Providing a coordinated series of MA compulsory and PhD summer courses aiming to familiarize students with the main trends and approaches in the field of communication and security governance in the European Union.
- Updating the teaching contents on the topic by research activities.
- Making aware students who do not automatically come into contact with EU studies of the importance of security governance by training them in using both the specialized language and methodology specific to subjects that pertain to the area of international relations, political sciences, as well as security studies.

The module's objectives will be achieved through the **teaching, researching and promoting** activities. To this respect, the EUSEGOV module includes a **two completely new courses**, one compulsory for MA students and one optional for PhD students, covering a major gap in the curricula i.e. the developments in the idea of European Security Governance. By bringing together academics and experts from various fields of knowledge, from civil society organizations and institutions, the interdisciplinary teaching and research approach of this Module provides the students with an in-depth and systematic understanding of key EU Security Governance topic. The EUSEGOV includes also research activities on the **Strategic communication in EU Security Governance thematic**. The research report will contain an extensive analysis of three aspects: *Strategic communication in EU – practices and official documents*; *EU Security strategic communication institutions*; *EU Security Governance future: alternative scenarios*.

A general dissemination campaign will be implemented to create a broad understanding of the importance and the particularities of EU Security Governance: two conferences, opening and closing conferences; a MA and a PhD round-table debates The main output is represented by the training of a target group formed by master students and PhD candidates in security and intelligence studies that must better understand the direct and indirect implications of EU's security governance impact on the member states.

DOMINOES

Digital cOMpetences InformatiOn EcoSystem[1]

ID: 2021-1-RO01-KA220-HED-000031158

The DOMINOES project aims to reduce societal polarization through combating the rapid spread of online disinformation among young people. In order to do achieve this result, the project aims to increase the capabilities of partner organizations to develop new and interactive online educational content, which is adapted to the specificities of the current and future, digitally skilled, generations of students. The project begins from two inter-related premises: that the digital ecosystem is undergoing a significant transformation, due to the emergence of new communication platforms and that higher education institutions need to develop curricula that teach critical thinking and digital skills holistically rather than in a disparate fashion.

The project targets two groups: current teaching staff and students of partner institutions, who will be future professionals in the

[1]This work was possible with the financial support of the ERASMUS + financial mechanism, through the project DOMINOES – Digital Competences Information Ecosystem, Contract Number – 2021-1-RO01-KA220-HED-000031158. The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

field of security and intelligence. Selected participants from the two target groups will be helped, through several on-site classes, to acquire digital teaching skills, to produce innovative educational material and to use advanced digital skills for the detection and countering of online propaganda, fake news and information manipulation.

The project will elaborate a handbook on the topic of digital disinformation and fake news. This will include the most relevant and up-to-date information on the evolution of the phenomenon of fake news, the psychology of disinformation, the social factors supporting or arresting the dissemination of fake news, skills relevant to avoid online disinformation and policies and legal approaches employed to deter the phenomenon. Then, three on-site courses, each including 30 participants, will take place in the three participating countries. A mix of professors and students will be taught how to avoid online disinformation and how to teach others to do so, in an interactive and inclusive fashion. Finally, the information gathered for the handbook and validated through the face-to-face interactions will be used for the creation of an online course which will be accessible to a wide audience and will represent a sustainable product of the project. This course will include not only the theoretical material gathered for the elaboration of the handbook, but also a wide set of interactive exercises aimed at facilitating student engagement with the material.

The main outcome of the project will be an increase in the advanced digital skills and ability to spot fake news of the representatives of the target group. Participants in the on-site and online courses will improve their teaching abilities and their competences in addressing a young generation of digital natives.

At the end of the project, the partners will organize three simultaneous multiplier events, which will be addressed to persons from the wider target group, but who were not part of the initial on-site training activities. The main results of the project will be presented, with a particular focus on the online training course. This will allow participants to access the same information as those that were included in the on-site activities and further help achieve the project's objectives of reducing societal polarization and combating online disinformation.

Erasmus+ Mobility Projects at "Mihai Viteazul" National Intelligence Academy

Between June 2020 and May 2022, two Erasmus+ KA103 mobility projects were implemented within „Mihai Viteazul" National Intelligence Academy (MVNIA). The projects were funded by the European Commission, through the National Agency.

The objectives pursued by MVNIA within the the two mobility projects were in line with the specific objectives of Key-Action 1. Therefore, the Academy sought to:

- Support students in order to improve their knowledge, skills and competences;
- Favour quality improvement, excellence in innovation and internationalization by intensifying transnational cooperation with other higher education institutions and training centers;
- Improve the international dimension of education and professional training by promoting mobility and cooperation between higher education institutions;
- Increase the capacity to offer study programmes that better meet the needs of the students.

The mobility of staff and students sets the premises for improving professional knowledge and experience, developing linguistic and intercultural skills, as well as strenghtening European identity through the promotion of common values. Collectively, the 2 projects encompassed a number of 8 beneficiaries, students and professors alike, who took part in different tyes mobilities, as follows:

- 4 training mobilities
- 2 traineeships
- 1 teaching mobility
- 1 study mobility

MVNIA embraces cooperation and recognizes the importance of belonging to university networks for the development of competitiveness and institutional modernization. For this reason, strenghtening existing partnerships and starting new projects are objectives of utmost importance in the process of institutional internationalization. Fortunately, the Erasmus programme has put at MVNIA's disposal all the mechanism needed to achieve this goal. As a result, throughout the implementaion period, the Academy has signed three new inter-institutional agreements with the following institutions: University of Malta, the Jagiellonian University in Krakow and Matej Bel University in Banska Bystryca.

Even though the two projects have been completed, the Academy will continue to disseminate and exploit their results in new projects, scientific publications, and by developing new study programmes.

Funded by
the European Union

INSET
CrItical Studies in INtelligence,
Technologies, and SEcuriTy Governance
(01.11.2022 – 31.01.2024)

INSET is an ERASMUS Mundus Design Measures project developed by a consortium of three universities: Mihai Viteazul National Intelligence Academy (Romania), University of Malta (Malta) and University Rey Juan Carlos (Spain) and financed by the European Commission (ERASMUS-EDU-2022-EMJM-DESIGN, code 101081354).

The aim of INSET is to develop a **joint master's program in Critical Studies in Intelligence, Technologies, and Security Governance**. The focus is on developing complex and interdisciplinary competences which are needed in understanding the dynamics of the 21st century world which is increasingly technology-based, hostile from a security perspective, and highly volatile.

INSET advances an inter- and multidisciplinary approach that combines critical studies in intelligence, security governance and technologies while bridging these areas of study and transfers specialized knowledge and competencies from specialists and practitioners in intelligence and security towards the civil society.

INSET joint MA programme's distinct novelty emerges from the following objectives:

1. it brings an interdisciplinary and multidisciplinary approach, which intersects the several concentrations under security

science: critical studies in intelligence, security governance, technologies;

2. it applies a critical approach to address contemporary security challenges and build a resilient security culture;
3. it is structured in a way that can be understood and assimilated by a wide variety of students, with different backgrounds: media studies, law, technology, political sciences, sociology, intelligence and security studies;
4. it goes beyond addressing these study areas in a disparate and segmented fashion, transversally focusing on their intersection, on their convergence, and on the manner in which they can synergically solve real societal problems.

INSET joint MA programme addresses the following educational gaps:

1. the need for a common European academic framework to assess security risks through technologically-driven intelligence production;
2. the underrepresentation of interdisciplinary master programs linking intelligence studies, security governance and technologies;
3. the rapid and recent evolution of perspectives on intelligence and security from traditional to more critical, interdisciplinary and reflexive ones;
4. the need to link intelligence studies and technological developments to society at large and to develop civil societies' abilities to analyse data, understand the functionality of technology, develop their digital competences;
5. the missing tools in addressing disinformation campaigns, part of hybrid warfare, that are shaping and reshaping democratic systems and affecting good governance practices, with little understanding or control from civil society.

As a **joint transnational and inter- and multidisciplinary master's program, INSET** encourages the internationalization of education via critical approaches to security issues and increases the capacity of partners to deliver joint educational programs. By providing a common framework and support for networking, it fosters academic cooperation among partners and, accordingly, it enhances the partners' capabilities to modernize their curricula and teaching practices. In line with the recent developments of both theoretical approaches (e.g. critical intelligence studies) and also the unprecedented technological challenges, the program aims to develop cutting-edge and labour market attractive skills for BA graduates with different backgrounds (e.g. law, technology, social and political science, intelligence, media studies). By providing academic excellence, INSET designs and implements the mechanisms needed for the delivery and functioning of a joint master's program.

The consortium is currently developing the organizational documents and the curriculum for the **joint master's programme INSET** with a view to enrolling the first cohort of students in the autumn of 2025. More information is available on the project website.

CALL FOR PAPERS *ROMANIAN INTELLIGENCE STUDIES REVIEW*

"Mihai Viteazul" National Intelligence Academy, via its National Institute for Intelligence Studies, publishes the *Romanian Intelligence Studies Review* (RISR), a high-quality peer reviewed and indexed research journal, edited in English and Romanian twice a year.

The aim of the journal is to create a framework for debate and to provide a platform accessible to researchers, academicians, professional, practitioners and PhD students to share knowledge in the form of high quality empirical and theoretical original research papers, case studies, conceptual framework, analytical and simulation models, literature reviews and book review within security and intelligence studies and convergent scientific areas.

Topics of interest include but are not limited to:

- Intelligence in the 21st century
- Intelligence Analysis
- Cyber Intelligence
- Open Source Intelligence (OSINT)
- History and memory in Intelligence
- Security paradigms in the 21st century
- International security environment
- Security strategies and policies
- Security Culture and public diplomacy

Review Process: RISR shall not accept or publish manuscripts without prior peer review. Material which has been previously copyrighted, published, or accepted for publication will not be considered for publication in the journal. There shall be a review process of manuscripts by one or more independent referees who are conversant in the pertinent subject area. Articles will be selected based on their

relevance to the journal's theme, originality and scientific correctness, as well as observance of the publication's norms. The editor evaluates the recommendation and notifies the author of the manuscript status.

The review process takes maximum three weeks, the acceptance or rejects notification being transmitted via email within five weeks from the date of manuscript submission.

Date of Publishing: RISR is inviting papers for No. 31 and 32 and which is scheduled to be published on June and December, 2024.

Submission deadlines: February 1st and July 1st

Author Guidelines: Author(s) should follow the latest edition of APA style in referencing. Please visit www.apastyle.org to learn more about APA style, and http://www.animv.ro for author guidelines. For more details please access the official website: **rrsi.ro**

Contact: Authors interested in publishing their paper in RISR are kindly invited to submit their **proposals electronically in .doc/.docx format at our e-mail address rrsi@sri.ro, with the subject title: article proposal.**

Appearing twice a year, the review aims to place debates in intelligence in an institutional framework and thus facilitating a common understanding and approach of the intelligence field at national level.

The target audience ranges from students to professionals, from the general public to those directly involved in intelligence research and practice.

ISSN - 2393-1450
ISSN-L - 2393-1450
e-ISSN 2783-9826

"MIHAI VITEAZUL"
NATIONAL INTELLIGENCE ACADEMY

20, Odăi Str.
Bucharest 1 - ROMANIA
Tel: 00 4037 772 1140
Fax: 00 4037 772 1125
e-mail: rrsi@sri.ro

www.animv.ro