No. 2 (34)/2025

ROMANIAN INTELLIGENCE STUDIES REVIEW

RISR No. 2 (34)/2025

ROMANIAN INTELLIGENCE STUDIES REVIEW

EDITURA ANIMV

EDITURA ANIMV

"MIHAI VITEAZUL"
NATIONAL INTELLIGENCE ACADEMY

ROMANIAN INTELLIGENCE STUDIES REVIEW

No. 2(34)/2025

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

Bucharest
2025

CONTENT

INTELLIGENCE IN THE 21ST CENTURY

THE STRATEGIC ROLE OF MANAGERIAL COMPETENCIES IN ENHANCING ORGANIZATIONAL RESILIENCE AND PERFORMANCE IN INTELLIGENCE ORGANIZATIONS

Marius-George PORUMBIȚĂ*

Abstract:

This article explores the relationship between managerial competencies and organizational performance, with a specific focus on intelligence organizations operating in highly complex and uncertain environments. Building on the theoretical models of managerial skills, the study integrates classical categories of competencies – technical, cognitive, and social – with modern dimensions such as emotional intelligence, social intelligence, and adaptability. The empirical research is based on a qualitative methodology, using semi-structured interviews with 18 managers from an intelligence institution. The analysis demonstrates that managerial performance is not the result of a single dominant competence, but rather of a dynamic equilibrium between multiple dimensions. Technical competencies provide credibility and ensure operational efficiency, while cognitive abilities enable strategic thinking and objective decision-making. Social and emotional competencies emerge as decisive in building trust, cohesion, and motivation within teams. Adaptability and continuous learning are identified as crucial for ensuring resilience and innovation in fast-changing contexts. The study also highlights critical limitations, such as the restricted sample size and the reliance on self-reported data. Overall, the findings confirm the necessity of shifting managerial evaluation and selection processes towards a more integrative approach that values relational and adaptive skills alongside professional expertise. The conclusions underline both the theoretical contribution to leadership studies and the practical relevance for strengthening organizational resilience and sustainable performance in intelligence settings.

Keywords: *managerial competencies; organizational performance; intelligence organizations; emotional intelligence; social intelligence; adaptability.*

---

* PhD Candidate, University of Bucharest and "Mihai Viteazul" National Intelligence Academy, E-mail: marius.porumbita@drd.unibuc.ro. Disclaimer: the material is a reflection of the authors' opinions and beliefs, and does not represent the opinions, policies or the views of the Romanian Intelligence Service or the National Intelligence Academy "Mihai Viteazul".

Introduction

Managerial competencies are one of the most important research topics in contemporary organizational sciences, having a direct impact on the performance and sustainability of institutions. In the context of accelerating economic, technological, and social changes, analysing how managers' skills influence organizational processes becomes essential. Intelligence organizations, characterized by complexity, uncertainty, and high decision-making pressure, provide a particularly relevant framework for investigating this relationship. This article aims to integrate theoretical perspectives and empirical findings on managerial competencies in order to identify the mechanisms through which they contribute to organizational performance and institutional resilience.

Managerial competencies and organizational performance: an integrative perspective

The study of managerial competencies has undergone significant development in recent decades, reflecting both the concerns of theorists and the practical needs of organizations to identify the factors that lead to sustainable performance. The literature has outlined several perspectives on the definition and classification of competencies, but their convergence highlights several common dimensions: knowledge, skills, behaviours, and attitudes that enable managers to effectively fulfil their roles and responsibilities (Boyatzis, 1982; Spencer and Spencer, 1993).

The first theoretical concerns emerged in the second half of the 20th century with the work of Katz (1955), who proposed the classic distinction between technical, human, and conceptual competencies. This structure formed the basis for further developments, such as the organizational competency models developed by Boyatzis (1982), which emphasized the correlation between managerial competencies and job performance.

In recent literature, Yukl (2011) developed a comprehensive model, frequently used in the analysis of managerial competencies, which includes six categories of competencies necessary for achieving performance. Three of these falls into the category of classic competencies: (1) technical competencies – knowledge and skills specific to the field of

activity; (2) cognitive competencies – strategic thinking, organizational diagnosis, ability to solve complex problems; (3) social competencies – communication, influencing, team motivation, relationship building.

Numerous other classifications proposed in the literature confirm the relevance of these categories. Spencer and Spencer (1993) developed a framework based on cognitive, social, and motivational competencies, and Boyatzis (2009) emphasized the role of emotional and social intelligence in determining managerial performance. Contemporary research emphasizes that these competencies are not static, but are dynamic resources that are activated differently depending on the situation and organizational context (Antonakis and Day, 2018).

In addition, Yukl added three modern competencies adapted to the requirements of contemporary organizations: (4) emotional intelligence – self-control, empathy, managing emotions in professional interactions; (5) social intelligence – the ability to understand and interpret group dynamics and social context; (6) the ability to learn from experience and adapt to change – cognitive flexibility and openness to new practices and perspectives (Yukl, 2011).

This model expands the classic paradigm of managerial competencies and integrates dimensions that are essential for effective management in organizations operating in complex and dynamic environments.

There is a growing consensus in the literature that managerial performance and, implicitly, organizational performance depend on the extent to which managers possess and effectively apply these competencies. Empirical studies (Luthans et al., 1988; Boyatzis, 2009; Yukl, 2013) show that high-performing managers are able to align their own and their team's competencies with the organization's objectives, use interpersonal skills to create cohesion and maintain the organizational climate, or develop robust decision-making processes that increase efficiency and reduce uncertainty.

Recent research confirms that there is no single competency that determines performance, but rather a configuration of competencies that, when adapted to the context, contributes to the achievement of objectives (Judge and Piccolo, 2004). Thus, cognitive and strategic competencies provide long-term vision, while interpersonal and emotional

competencies are essential for effective strategy implementation and maintaining employee motivation. High-performing managers are distinguished by their ability to mobilize and combine different sets of competencies in a process of continuous adaptation to the complexity and dynamics of the environment. This direct link between competencies and performance is confirmed by numerous empirical studies and forms the basis of applied research in highly complex organizations.

Managerial competencies as determinants of performance in intelligence organizations

Intelligence organizations are distinguished by a working environment characterized by uncertainty, high pressure, incomplete information, and the need to make quick decisions, often with major strategic impact (Treverton, 2009). In these organizations, managers not only coordinate day-to-day activities, but also shape complex analytical processes, manage sensitive resources, and create cohesion in teams under constant stress.

Research on intelligence management is relatively limited compared to other fields, but the existing literature highlights that organizational performance depends on a distinct set of managerial skills, tailored to the specifics of this type of organization (Walsh, 2016; Oleson and Cothron, 2016).

Cognitive and analytical skills. A first fundamental pillar for intelligence managers is cognitive and analytical skills. These include the ability to evaluate ambiguous information, identify patterns in incomplete data, and anticipate possible scenarios (Heuer, 1999). Studies show that managers who possess these competencies enhance the quality of analytical products and reduce systematic errors in judgment. Also, the ability to prioritize information and integrate multiple perspectives is essential for transforming raw data into strategic knowledge (Marrin, 2007). Oleson and Cothron (2016) emphasize that flexible, continuous learning-oriented management improves the accuracy of intelligence products and reduces organizational vulnerability.

Technical and professional skills. Technical skills in intelligence organizations refer not only to knowledge of the specific field (geopolitics, security, technology, etc.), but also to the use of advanced data collection

and analysis technologies (Walsh, 2016). High-performing managers are able to integrate new technologies into analysis processes and ensure that staff are trained to use them effectively.

Social and coordination skills. Another key category is social skills – the ability to communicate clearly, build collaborative networks, and coordinate multidisciplinary teams. Walsh (2021) shows that modern intelligence organizations are required to develop new governance mechanisms, which requires increased negotiation and collaboration skills. Within the Five Eyes alliance (US, UK, Canada, Australia, New Zealand), information sharing was only effective to the extent that managers demonstrated collaborative leadership skills (Walsh, 2011).

Emotional and social intelligence. The literature confirms that, under conditions of stress and continuous pressure, emotional intelligence is crucial for maintaining balance and resilience in teams (Caruso and Salovey, 2004). Managers who are able to regulate their own emotions and understand the reactions of team members create a climate of trust, which leads to better staff retention and increased quality of analysis. Jenkins (2018) points out that these skills become even more important in the context of virtual leadership and the use of digital collaboration platforms.

In addition, social intelligence is necessary to interpret group dynamics, to negotiate between multiple stakeholders: governments, agencies, national or international partners; and to build organizational legitimacy. Hatfield (2008) emphasizes that succession in the intelligence management hierarchy depends not only on expertise, but also on the ability to develop credible relationships and trusted networks.

The ability to learn and adapt. In an environment marked by rapid change, the ability of managers to learn from experience and adapt is one of the most important competencies (Yukl, 2011). Recent studies show that intelligence organizations that promote organizational learning and managerial flexibility are more resilient in the face of new threats (Phythian, 2013). Walsh (2021) shows that without mechanisms for continuous manager development and adaptive governance, intelligence agencies risk losing their relevance and ability to respond effectively to new challenges.

The performance of intelligence organizations depends on the ability of leaders to combine classic skills – cognitive, technical, and social with modern ones – emotional, social, and adaptive. Failure to develop and evaluate these skills leads to structural vulnerabilities: erroneous analyses, loss of trust, and decreased ability to cooperate with other institutions. Succession planning and continuous development become strategic imperatives: without training and transfer mechanisms, intelligence organizations remain fragile in the face of change.

Thus, managerial competencies in intelligence can no longer be viewed as mere individual skills, but as critical resources for organizational and national security. High-performing managers are those who manage to combine analytical, technical, and social skills with flexibility and adaptability, creating resilient organizations capable of coping with the complexity and volatility of the contemporary security environment.

Qualitative analysis methodology

The research was conducted in a military intelligence organization – with a military structure and hierarchy – within an analytical structure responsible for producing and integrating analytical products. The organization is characterized by formal rules, developed bureaucracy, and a sustained process of structural and cultural transformation, with direct effects on managerial practices and the human resource profile. This context required a qualitative methodological approach, capable of capturing the nuances of managerial behaviours and competencies in relation to performance.

The target population included 58 managers of the organization: level 1 – heads of executors; level 2 – heads of heads of executors, with central and territorial representation. Strategic management was excluded from the analysis. Based on a systematic algorithm: alphabetical listing on four sampling frames level 1/2 × central/territorial, selection from position 2 with step 4, 18 participants (≈31% of the population) were selected: 13 level 1 managers (8 central, 5 territorial) and 5 level 2 managers (3 central, 2 territorial). The sample structure ensured very good coverage of the main socio-demographic and organizational dimensions relevant to the research objectives.

We used a semi-structured interview, built on a "funnel" model (from general questions to specific questions), and organized into four thematic blocks: (1) performance in the organization; (2) managerial behaviours and competencies; (3) team characteristics; (4) organizational context. The guide contained only open-ended questions and was accompanied by documentation for operators (managerial performance, competencies, behaviour, and synopsis of contingency theories). This configuration allowed us to capture the causal mechanisms and perspectives of the actors on the competency-performance relationship in the studied environment.

The interviews were conducted at the organization's headquarters in August–September 2022, face to face; each interview lasted 90-120 minutes. The process was carried out with the support of two interviewers (sociologists), which generated minor differences in style: one interviewer followed the guide more strictly, while the other introduced clarifications and contextual questions. All interviews were transcribed in full, then subjected to thematic coding and aggregation into categories congruent with the study's objectives.

Gary Yukl's model (2011) – structured around technical, cognitive, and social competencies, emotional intelligence, social intelligence, and learning and adaptability – served as the theoretical framework for interpreting the data.

The qualitative design, focused on a single analytical structure within a military intelligence organization, limits the statistical generalization of the results. The differences in style between the two operators represent a potential source of variation in the depth of responses, mitigated by the standardization of the guide and full transcription. At the same time, the sensitivity of the organizational environment can sometimes limit the level of detail in reports.

Managerial competencies and their impact on organizational performance – case study

This analysis aims to explore in depth the relationship between the dimensions identified in the literature – technical, cognitive, and social skills, emotional intelligence, social intelligence, and the ability to learn and adapt – and the level of performance perceived in the

organization studied. By integrating data obtained from interviews with managers and correlating them with established theoretical models, the chapter highlights not only the relevance of each category of skills, but also how they interact to support long-term organizational performance.

Technical competencies. Technical competencies are the traditional foundation of any managerial career and have historically been considered the basic criterion for selecting leaders. In the organization studied, the emphasis on these competencies was noted by many of the interviewees, who emphasized that a manager's legitimacy derives largely from their level of knowledge of the activity they coordinate. Analysis of the interviews reveals that, although their importance is not disputed, there is a growing awareness that they are not sufficient to ensure lasting organizational performance.

A mechanism linking technical skills and performance is professional credibility. Managers who do not demonstrate an understanding of the specific processes in their field risk being perceived as lacking authority. For example, one of the respondents (M2) argued that "he would never encourage the idea of having as a manager someone who lacks professional skills or who has not demonstrated, through their work, that they know their job." This observation is consistent with Yukl's theory, according to which technical knowledge gives leaders the ability to understand the specifics of the work and to lead the team in a realistic and credible manner. Without this foundation, managers face a rapid erosion of trust among their subordinates.

Another effect associated with technical skills is the ability to accurately assess tasks and resources. Well-trained managers can more easily identify obstacles, anticipate bottlenecks, and formulate realistic requirements for the team. M13 emphasizes this dimension by stating that a leader must "understand the objective difficulties of the work," which requires knowledge of internal processes and technological limitations. Thus, technical skills directly contribute to avoiding poor decisions that could lead to frustration and demotivation among subordinates.

A lack of technical knowledge can expose the leader to a loss of respect and credibility. Even if their main role is no longer one of execution but of coordination, managers must periodically demonstrate

that they have a grasp of the essence and e of the team's activities. Otherwise, the difference between them and their subordinates becomes a factor of vulnerability.

Analysis of the interviews also reveals a much more important nuance: technical skills cannot function in isolation. Several respondents noted that a manager who is an expert but lacks social or cognitive skills fails to generate collective performance. M4, for example, states that of the three major categories (technical, cognitive, social), he would sacrifice the first two, as they can be acquired relatively easily through training and experience. This view reflects a paradigm shift: while in the past the focus was almost exclusively on professional expertise, there is now an awareness that relationships and adaptability have a more direct impact on organizational results.

In conclusion, technical skills are recognized by the managers interviewed as necessary but not sufficient. They are the starting point for managerial legitimacy, but they cannot alone ensure organizational performance. Thus, their role is to underpin and support the other categories of competencies, which become decisive in differentiating between high-performing and low-performing managers.

Cognitive competencies. Cognitive competencies are a fundamental category in Gary Yukl's model, being associated with the ability to analyse complex information, make connections, develop creative solutions, and plan strategically. Interviews with managers in the organization studied confirm the importance of these competencies, but at the same time highlight differences in perception regarding their weight in relation to other types of skills.

A first central aspect highlighted is the role of cognitive skills in increasing managers' adaptability to the complex environment in which they operate. Manager M7 places these skills at the top of his hierarchy, arguing that "if you have these cognitive qualities, you adapt much more easily to the environment, you are predisposed to fit in anywhere." We thus find that a high level of analytical and logical thinking allows for rapid integration into variable contexts, which leads to better organizational performance. In modern organizations, where change is a constant, this ability to adapt becomes a decisive competitive advantage.

Another finding shows that cognitive skills are an essential filter through which knowledge becomes useful and operational. In the same vein, M8 emphasized that "if you don't have the brains, there's no point in learning a lot." This direct statement shows that the accumulation of technical knowledge is not enough if there is no solid cognitive basis to enable its processing and application.

Another causal mechanism observed is the ability to analyse and plan strategically. M3 mentions that although analytical skills are not always present, when they are, they are a great advantage for managers. This observation suggests that managerial performance is often enhanced by the ability to correlate disparate information and formulate clear courses of action. Similarly, M10, reflecting on his own professional career, emphasizes the importance of consistency and the ability to maintain "the determination to keep the bar high every day," traits that derive from a cognitive pattern oriented toward rigor and organization.

The interviews also reveal differences between hierarchical levels. Senior managers tend to place greater emphasis on cognitive skills, considering that they facilitate the connection between different organizational levels. For example, M3 states that, with the transition from line management to senior management, social skills become more important, but cognitive ability remains central to supporting coordination and analysis processes. This finding suggests that, at strategic levels, logical thinking and long-term vision become critical factors for success.

Another element of interpretation is provided by M13, who emphasizes that a lack of structural thinking affects the decision-making process: "if you get attached to a person and decisions are altered by affinities, performance declines." Here, cognitive skills act as a filter of objectivity, allowing the manager to distance themselves from emotional or subjective factors and make decisions that support organizational goals. Without this filter, performance is sacrificed to personal biases.

Interviewees also refer to accelerated learning ability, which is directly linked to cognitive skills. Managers perceive that the ability to quickly understand a new field and integrate complex information allows them to gain professional recognition and inspire confidence among their team. M17 exemplifies this point, recounting how she had to

develop accounting comprehension skills in order to manage documents with legal and financial implications. This experience shows that performance is not only determined by prior training, but also by the cognitive ability to learn quickly and apply new knowledge.

In conclusion, cognitive skills are perceived by the managers interviewed as an essential pillar of performance. They cannot completely replace technical or social skills, but they play a crucial role in integrating and capitalizing on them. High-performing managers are those who manage to combine analytical thinking, foresight, and objective decision-making, thus generating a solid foundation for organizational development and achieving sustainable long-term results.

Social skills. Social skills are the dimension most frequently mentioned by the managers interviewed, as they are perceived as fundamental to ensuring organizational performance. While discussions on technical and cognitive skills were more nuanced, there was almost unanimous consensus on social skills: without them, a manager cannot mobilize the team and achieve sustainable results.

A first aspect highlighted is the ability to build relationships based on trust and mutual respect. Manager M1 states that the essence of a successful leader lies in "compromise, the ability to work with others and not to close doors when it is not necessary." This perspective suggests a clear causal mechanism: social skills facilitate the maintenance of long-term relationships, the avoidance of conflicts, and the creation of a stable organizational climate. Without them, the team becomes fragmented and collective performance is affected.

Another important element is the ability to communicate effectively and persuasively. M6, which gives social skills a 50% weighting in its hierarchy of priorities, states that they are the "essential ingredient" of leadership. Clear and convincing communication allows the manager to convey objectives, provide constructive feedback, and create a sense of cohesion. This ability is not just a communication skill, but a tool for mobilising and motivating, without which the team can become disoriented.

Another significant causal mechanism is the role of social skills in preventing and managing conflicts. M14 emphasizes that a successful manager is "with people, not above them." This wording highlights

the importance of a relationship of proximity and partnership, which reduces tensions and discourages conflictual behaviour. In an environment where relationships are based on authoritarianism and a lack of dialogue, demotivation, voluntary departures, and decreased productivity quickly arise.

The theme of recognition and appreciation of subordinates also appears in the interviews. M12 states that "a good manager knows how to see the person behind the job and appreciate them for their efforts." This observation suggests that organizational performance depends not only on objective processes, but also on how valued employees feel. Social skills act as a catalyst for intrinsic motivation, which leads to increased engagement and loyalty to the organization.

In addition, M9 offers an indirect perspective on social skills through performance indicators: "the number of subordinates who ask to leave may be a signal of leadership quality." This shows that a lack of social skills has direct and quantifiable consequences on team stability. Excessive staff turnover caused by poor relations with the manager is a cost and vulnerability factor for the organization.

In conclusion, the analysis shows that, for the organization studied, social skills are the strongest predictor of managerial performance. While technical skills confer legitimacy and cognitive skills support rational decision-making, social skills are what bring life and cohesion to the team. High-performing managers are those who manage to be close to people, understand them, and mobilize them through a participatory and empathetic leadership style. Without these skills, even leaders who are highly trained technically or cognitively face failure because they fail to generate the collective motivation necessary to achieve organizational performance.

Emotional intelligence. Emotional intelligence is a set of essential skills for managers who want to lead high-performing teams in a sustainable way. This includes empathy, emotional self-regulation, self-awareness, and the ability to express feelings in an authentic and constructive way. The interviews show that, although not all managers explicitly use the term "emotional intelligence," most refer to its constituent elements, confirming the relevance of this dimension in organizational practice.

A first causal mechanism highlighted is empathy as a factor of cohesion. M12 emphasizes that "you have to care about human aspects beyond professional tasks." This statement suggests that a manager who understands the states, emotions, and difficulties of their employees can create a climate of trust and openness. Without this empathy, the team risks alienation, lack of motivation, and even voluntary departures.

Another element is emotional self-regulation. M18 notes that managers who lack the ability to manage their emotions can become "absent and underperforming," even if they have solid technical skills. This observation illustrates that a leader who cannot control their reactions in stressful or conflictual situations conveys instability to the team, generating insecurity and a decline in collective performance. In contrast, managers who remain calm and balanced under pressure provide a positive model of resilience.

Self-awareness is also implicitly mentioned by several interviewees. M6, for example, states that "a manager must be concerned about the impact they have on their people." This concern shows an understanding of one's own emotions and behaviours and how they influence the team. Thus, emotional intelligence acts as a self-monitoring tool, allowing the leader to adjust their communication style and avoid tense situations.

Another relevant causal mechanism is the ability to motivate through emotional support. M1 mentions that "the difference between high performers and low performers is how they know how to manage interpersonal relationships." Therefore, a manager with a high level of emotional intelligence does not limit themselves to delegating tasks, but supports employees when they face personal or professional difficulties. This attitude increases employee motivation, involvement, and loyalty, directly contributing to increased organizational performance.

In addition, M14 emphasizes the importance of authenticity and emotional congruence, arguing that "the impact is very high when people feel that the manager is sincere and transparent." This confirms that, beyond cognitive and technical skills, emotional authenticity strengthens the relationship of trust between the leader and the team.

In conclusion, emotional intelligence proves to be a key factor in achieving organizational performance. The managers interviewed recognize that empathy, self-regulation, and authenticity are indispensable

for maintaining a healthy climate and mobilizing teams toward common goals. The absence of this dimension leads to alienation, conflict, and the loss of valuable human capital, while its presence contributes to strengthening cohesion and achieving sustainable results.

Social intelligence. Social intelligence is defined in Gary Yukl's model as the ability to understand situational demands and adopt behaviours appropriate to the context. It combines social perception – the ability to read and understand the organizational environment, with behavioural flexibility – the ability to adjust leadership style according to the situation. Interviews with managers of the studied organization confirm the importance of this dimension, even if not all of them explicitly use the term "social intelligence."

A first aspect highlighted is the need for flexibility in interpersonal relationships. M4 states that "mental flexibility determines relational flexibility," emphasizing that managers must be able to deal with different types of people and contexts. This causal mechanism is essential: rigidity in behaviour generates tension and resistance to change, while flexibility allows for continuous adaptation and maintenance of efficiency.

Another mechanism identified is the ability to calibrate leadership style according to context. M17 describes underperforming leaders as characterized by "fear of failure" and a tendency to over control. This reflects a lack of behavioural flexibility, which leads to blockages and inhibits creativity in the team. In contrast, leaders with high social intelligence know how to alternate between a more directive and a more participatory style, depending on situational needs.

Manager M15 emphasizes the role of social intelligence in harmonizing relationships between hierarchical levels. Managers who can understand organizational dynamics and adjust their behaviour according to their interlocutor manage to build bridges between departments and facilitate cooperation. This type of behaviour has direct effects on overall efficiency, reducing conflicts and communication barriers.

Another element highlighted in the interviews is the ability to anticipate social reactions. Managers with developed social perception can assess the potential impact of a decision on the team and adapt the implementation method to minimize resistance. Thus, social intelligence

is not limited to specific interactions, but plays a strategic role in creating a climate of acceptance and involvement.

In conclusion, social intelligence is an essential dimension for managers in the organization studied, even if it is less frequently mentioned explicitly. It acts as a link between cognitive, emotional, and social skills, allowing leaders to adjust their behaviour and navigate complex and variable contexts effectively. Managers with a high level of social intelligence are able to reduce tensions, facilitate cooperation, and increase the organization's adaptability, which has a direct impact on long-term performance.

Ability to learn and adapt. The ability to learn from experience and adapt to change is the last of Yukl's categories, but it is one of the most important dimensions for ensuring long-term organizational performance. In today's dynamic environment, characterized by rapid change, emerging technologies, and external pressures, managers can no longer rely solely on accumulated experience but must demonstrate flexibility and a constant willingness to adjust their behaviours and strategies. The interviews confirm that this ability is perceived as a fundamental condition for managerial success.

One aspect that stands out is the inclination toward continuous development. M5 states that a successful leader must have "a desire for constant development and a focus on learning." This element indicates that performance is not limited to the accumulation of initial expertise, but involves a process of continuous improvement. The lack of this orientation leads to stagnation and an inability to respond to the ever-changing demands of the organization.

Another mechanism observed is learning from negative experiences. M16 emphasizes that "negative examples motivated me to be different." This statement shows that learning does not derive exclusively from successes, but also from failures or critical observations. Managers who are able to extract lessons from difficult situations manage to adjust their strategies and prevent mistakes from being repeated, which leads to an increase in organizational efficiency.

At the same time, M17 emphasizes the importance of an open attitude toward learning, arguing that "high-performing managers are those who accept that they always have something to learn." This

perspective indicates a cause-and-effect mechanism in which cognitive modesty and willingness to accumulate new information contribute to maintaining relevance and competitiveness. Managers who think they "know everything" risk becoming rigid and losing touch with organizational realities.

Another important element is the ability to adapt to environmental changes. M13 shows that managerial success depends on the ability to adapt to requirements and respond appropriately to new challenges. In dynamic organizations, adaptability translates into innovation, the ability to rethink processes and introduce creative solutions, which directly contributes to long-term performance.

In conclusion, the ability to learn and adapt is perceived by managers in the organization studied as an essential skill for managerial success. It allows leaders to turn change into opportunity and prevent rigidity, thereby contributing to organizational resilience. High-performing managers are not those who never make mistakes, but those who manage to learn from experience and constantly adjust their mental models and strategies. Without this dimension, organizations risk becoming vulnerable to external changes and losing their capacity for innovation.

The analysis of interviews with managers in the studied organization, through the lens of the six categories of competencies identified by Gary Yukl, reveals a complex and nuanced picture of managerial performance. The central conclusion is that none of these categories is sufficient on its own to guarantee success, but their combination, in a dynamic balance, is the key to sustainable performance.

Technical competencies form the basis of professional legitimacy, providing managers with the necessary credibility in the eyes of their subordinates. They enable realistic assessment of tasks and resources and help to avoid managerial errors. However, when not coupled with cognitive and social skills, they remain insufficient, leading only to a minimum level of organizational functionality.

Cognitive skills complete this picture, being essential for analysis, planning, and objective decision-making. Managers who excel at this level can learn quickly, anticipate the consequences of decisions, and

formulate clear strategic directions. Without them, the organization risks facing rigidity and a lack of vision.

Social skills are emerging as the decisive factor for performance. They enable the building of trusting relationships, team mobilization, and the maintenance of internal cohesion. Managers who fail to communicate effectively, manage conflict, and recognize the merits of their subordinates' risk generating demotivation, excessive staff turnover, and a decline in collective involvement.

Emotional intelligence complements this relational dimension, being a factor of stability and motivation. Empathy, emotional self-regulation, and self-awareness contribute to creating a healthy organizational climate and strengthening team resilience. Without these skills, even technically and cognitively competent managers can become ineffective due to their inability to maintain the emotional engagement of the team.

Social intelligence acts as a glue between all these dimensions, allowing leaders to adjust their behaviours to the context and harmonize relationships across hierarchical levels. Behavioural flexibility and the ability to anticipate social reactions ensure more effective implementation of decisions and reduce organizational tensions.

The ability to learn and adapt provides the necessary foundation for organizational resilience. Managers who are open to learning, who turn negative experiences into constructive lessons, and who constantly adjust their strategies become vectors of change and innovation. Without this ability, the organization risks becoming vulnerable to external changes and losing its competitiveness.

The overall analysis shows that organizational performance is the result of a balance between technical, cognitive, social, and adaptive dimensions, with a major emphasis on social and emotional ones. While in the past the selection of managers was based predominantly on professional expertise, it is now becoming clear that interpersonal skills, empathy, and flexibility are the determining factors for success. In the organization studied, high-performing managers are described as those who manage to combine technical knowledge and analytical thinking with the ability to be close to people and to learn continuously.

In conclusion, organizational performance does not depend on excellence in a single category of competencies, but on the interaction and complementarity of all six. Managers who manage to achieve this balance become authentic leaders, capable of inspiring confidence, creating cohesion, and guiding the organization toward sustainable long-term results.

Critical analysis of data and assessment of research limitations

Analysis of the interviews conducted highlights a number of converging trends in managers' perceptions of the competencies required for organizational performance. Respondents consistently emphasized the importance of social competencies (communication, empathy, the ability to build relationships and manage teams), considering them either complementary to or even superior to professional or cognitive competencies. This finding is relevant, given that, in historical organizational practice, managerial selection has been based predominantly on professional skills and psychometric assessments.

However, the responses indicate a diversity of perspectives: some interviewees place cognitive skills – mental flexibility, analytical and anticipatory abilities – first, while others believe that professional experience remains the foundation without which performance cannot be achieved. This plurality of opinions reflects a complex reality: managerial performance is not based on a single type of competence, but on a balance between professional, cognitive, and social dimensions.

A critical aspect revealed by the data is the lack of a strong correlation between the official criteria for managerial selection and the realities of organizational performance. Interviewees point out that standardized testing or seniority criteria cannot capture the social skills and leadership attitudes that prove decisive for team cohesion. In this sense, the data confirms a tension between the traditional selection paradigm based on "technical expertise" and the current need for relational leadership.

Furthermore, a comparative analysis of the responses shows that, in the interviewees' perception, underperforming managers are characterized by rigidity, lack of involvement, poor communication, lack

of empathy, and inability to motivate subordinates. In contrast, managers considered to be high performers are distinguished by flexibility, openness, the ability to delegate, and to integrate multiple perspectives. A dichotomy between authoritarian and participatory styles is therefore emerging, with an obvious advantage for the latter.

Although the interviews provide a detailed picture of managerial perceptions, the research has some methodological limitations that should be mentioned: (1) sample size – the relatively small number of respondents and their origin from a single organization limit the degree of generalization of the conclusions; (2) the subjectivity of the responses – as these are self-assessments and perceptions of colleagues, there is a risk of distortions generated by personal experiences or the desire to project a favourable image; (3) absence of methodological triangulation – the analysis is based exclusively on qualitative interviews, without being corroborated by other data sources (performance evaluations, organizational indicators, direct observation); (4) limited contextualisation – the responses reflect a particular organisational framework, which limits the applicability of the conclusions to organisations with different managerial cultures or leadership systems; (5) lack of a consensual hierarchy – although most interviewees recognized the central role of social skills, there is no uniform hierarchy among the three categories of traditional skills, suggesting that managerial performance depends on multiple contextual variables.

Conclusions and recommendations

The analysis highlighted that managerial performance in military intelligence organizations is the result of a complex interaction between competencies, behaviours, and organizational context. Managerial competencies do not act in isolation but function through causal mechanisms that integrate technical, cognitive, social, and emotional dimensions.

The assessment shows that managerial performance cannot be reduced to a single set of competencies, but requires a balance between professional, cognitive, and social dimensions. Even though managerial

selection has traditionally been based on technical expertise and psychometric assessments, current data indicates an increasing need for relational leadership and social skills capable of building trust, motivating teams, and generating organizational cohesion.

At the same time, managers' perceptions suggest that rigidity, lack of involvement, and communication deficiencies are the main factors limiting performance, while flexibility, openness, and adaptability define the profile of a successful manager. This conclusion confirms the transition from an authoritarian to a participatory paradigm, in which managerial success depends on the quality of interpersonal relationships at least as much as on professional expertise.

The conclusions are in line with international findings in the literature on transformational leadership and contingency theories, which show that performance is determined by the fit between managers' behaviours and situational characteristics. At the same time, the study contributes to the literature by contextualizing these theories in the environment of intelligence organizations in Romania, an area that has not been explored academically.

Based on the data analysed, we can say that high-performing managers are those who combine technical expertise with social and emotional intelligence, adopting a flexible and adaptive leadership style. They manage to mobilize human resources within a strict hierarchical framework, but also to cultivate an organizational climate based on trust and collaboration, which generates sustainable performance.

These results not only confirm existing theories, but also have practical implications for the development of managerial resources: the selection, training, and evaluation of managers must simultaneously target technical, cognitive, and socio-emotional skills, depending on the specific context of the organization. In this way, both short-term efficiency and long-term resilience and adaptability of military intelligence organizations can be ensured.

The research results indicate the need for an integrated approach to the development of managers in military intelligence organizations, by strengthening the balance between technical and social skills, implementing training programs adapted to hierarchical levels, promoting

an organizational climate based on trust and collaboration, making leadership styles more flexible depending on the situational context, continuous investment in the development of cognitive skills – analysis, critical thinking, decision-making –, and the use of multidimensional evaluation mechanisms that capture both operational performance and the impact on team cohesion and organizational climate.

References:

1. Antonakis, J., and Day, D. V. (2018). *The nature of leadership* (3rd Ed.). SAGE Publications.

2. Boyatzis, R. E. (1982). *The competent manager: A model for effective performance*. Wiley.

3. Boyatzis, R. E. (2009). Competencies as a behavioural approach to emotional intelligence. *Journal of Management Development, 28*(9), 749-770. https://doi.org/10.1108/02621710910987647

4. Caruso, D. R., and Salovey, P. (2004). *The emotionally intelligent manager*. Jossey-Bass.

5. Hatfield, R. (2008). "Leadership succession planning in intelligence organizations." *American Intelligence Journal, 26*(1), 2-8.

6. Heuer, R. J. (1999). *Psychology of intelligence analysis*. Centre for the Study of Intelligence.

7. Jenkins, J. (2018). Ethical leadership in the U.S. intelligence community. *Journal of Leadership Studies, 12*(1), 59-73. https://doi.org/10.1002/jls.21561

8. Judge, T. A., and Piccolo, R. F. (2004). Transformational and transactional leadership: A meta-analytic test of their relative validity. *Journal of Applied Psychology, 89*(5), 755-768. https://doi.org/10.1037/0021-9010.89.5.755

9. Katz, R. L. (1955). Skills of an effective administrator. *Harvard Business Review, 33*(1), 33-42.

10. Luthans, F., Hodgetts, R. M., and Rosenkrantz, S. A. (1988). *Real managers*. Ballinger.

11. Marrin, S. (2007). Intelligence studies: The development of a discipline. *Journal of Intelligence History, 5*(1), 1-14. https://doi.org/10.1080/16161262.2007.10555117

12. Oleson, P., and Cothron, T. (2016). "Leadership challenges in the U.S. intelligence community." *American Intelligence Journal, 34*(2), 29-37.

13. Phythian, M. (2013). *Intelligence theory: Key questions and debates*. Routledge.

14. Spencer, L. M., and Spencer, S. M. (1993). *Competence at work: Models for superior performance*. Wiley.

15. Treverton, G. F. (2009). *Intelligence for an age of terror*. Cambridge University Press.

16. Walsh, P. (2011). Intelligence leadership in practice: Insights from the Five Eyes. *Intelligence and National Security, 26*(1), 1-25. https://doi.org/10.1080/02684527.2011.534079

17. Walsh, P. (2016). Intelligence leadership after 9/11. *Intelligence and National Security, 31*(2), 245-268. https://doi.org/10.1080/02684527.2014.988445

18. Walsh, P. (2021). Leadership and integrity in intelligence organizations. *Intelligence and National Security, 36*(2), 165-182. https://doi.org/10.1080/02684527.2020.1859989

19. Yukl, G. (2011). *Leadership in organizations* (7th Ed.). Pearson.

20. Yukl, G. (2013). *Leadership in organizations* (8th Ed.). Pearson.

IMPLICATIONS OF ARTIFICIAL INTELLIGENCE FOR INTELLIGENCE ORGANIZATIONS IN THE CONTEXT OF GLOBAL SECURITY TRANSFORMATIONS

Mihai CIOBANU*

Abstract:
The period in which artificial intelligence (AI) was treated in a speculative way in the field of national security appears to be over. The current dynamics on the geopolitical stage generated new technological needs which stimulated innovation even further, contributing to an increased inter-play between supply and demand. Between 2023 and 2025 AI moved from image and video generation to broader and more interactive environments, all in the light of new players and new models joining in the race. This article synthesizes developments and assesses the implications of AI advancement over national security and especially over intelligence agencies. The acceleration of AI capabilities and global reactions over large-scale deployment have prompted intelligence agencies to explore the implications for national security and have also led to organizational changes. AI is truly an agent of change, with the potential to bring organizational transformations in intelligence work, all while also being an agent of multiplication and creation of new risks, both external and internal, for national security agencies.

Keywords*: artificial intelligence; national security; intelligence; Geopolitics; technology; transformation.*

Introduction

AI's accelerated development is reshaping the national security and the everyday practice of intelligence. Generative systems now produce not only text and images but also video, interactive digital environments and applications designed for specific tasks. All of these

* PhD candidate, "Mihai Viteazul" National Intelligence Academy Bucharest, email: ciobanu.mihai@animv.eu. Disclaimer: the material is a reflection of the authors' opinions and beliefs, and does not represent the opinions, policies or the views of the Romanian Intelligence Service or the National Intelligence Academy "Mihai Viteazul".

developments affect how data is collected, processed and used, at a scale and speed that exceeds human capacity. In addition, there is also a need to protect data. For intelligence agencies, AI represents a dual challenge: on one hand, it increases the volume and quality of collection and analysis processes and on the other hand, it is a catalyst for new vulnerabilities: through the public exposure of sensitive information, new types of cyber-attacks, disinformation and influence operations. In this article we will refer to developments from 2023 to the first part of 2025. During this period, the *DeepSeek* episode was a global stress test for governments and regulators in the western world. Our aim is to identify and analyse various factors that make up the problems that intelligence agencies must manage in relation to AI development and deployment. At the same time, we will focus on operational and organizational implications for intelligence agencies, brought by these factors. Finally, we will explore the perspective of congruence and intersections between AI and the intelligence domain. The text relies both on an analysis of the specialized literature, using techniques specific to the content analysis and semantic meta-analysis method, as well as on our observations during the research.

Accelerating the evolution of AI capabilities

To talk about AI just a few years ago meant to talk about emergence. The advancements brought by competition led to a very fast paced evolution of AI capabilities. If the year 2023 was associated with text and image generation at a very wide scale, 2024 brought rapid progress in video and music generation. By early 2025, both research and industry shifted their interest and concern towards connecting different environments in an interactive matter, the best example being the possibility of creating playable game experiences from 2D sketches. This tendency alone is an indicator that content generation is experimenting with the convergence of planning and drafting with simulation (O'Donnel, Heaven, and Heikkilä, 2025). Of course, these kinds of shifts are enabled by development and improvements in hardware, expanding the feasible size and responsiveness of AI models, making way for new functionalities.

In parallel with the AI industry and as a natural response to technological advance, organizations started reframing their approach to operating with huge amounts of data. The literature notes an increased interest in tools that perform specific tasks, whose impact is quantifiable in various professional environments. Intelligent functionalities are increasingly related to workflows and workload and less to generic content generation (Davenport and Bean, 2025).

Davenport and Bean (2025) identify five trends for AI in 2025 that place emphasis on:

1. reassessing the promises of the industry regarding capabilities and advancements of AI models and agents;
2. moving from perception-based enthusiasm to systematic evaluation of generative AI;
3. prioritizing new data production and its management;
4. investing in leadership and governance models regarding managing lots of data and AI models;
5. clarifying responsibilities and implementing oversight across organizations in regard to AI models use.

An equally significant trend has been noted in the gradual shift of organizations toward what is now known as data-driven cultures. Davenport and Bean (2025) noted that 2024 marked a doubling in the number of companies that prioritized AI data management and AI training data management, establishing practices in this regard, The same authors noted that 2025 brought a slowdown, with only 33% of the companies maintaining the same pace of establishing internal policies and cultivating a culture related to AI implementation. A survey cited by the same authors showed that cultural and the management of change remained the primary obstacles in consolidating AI adoption by individuals. This indicates, of course, that the success of AI integration is not only dependent on innovation, but on the ability of organizations to reshape their own cultures and workflows as well. Domanska (2025) emphasizes that in the very close future organizations will need to appoint specialized AI officers who should watch be responsible for the implementation of AI and for formulating and changing principles and procedures regarding the use of AI in their organizations.

The overall picture is one in which AI models (and maybe AI agents in the near future) and organizational practices need to co-evolve and adapt to one another. As AI models demand broader, higher-quality data, organizations must increase investment in quality assurance and data security, as well as adapt the management perspective. The co-integration of these components directly affects the feasibility and the quality of deploying AI within intelligence agencies, where ownership, availability, reliability and timeliness of data are crucial. The rapid pace of AI development became visible not only in the market or in the industry but also in public reactions across the globe.

Global architects of public policies on AI

Progress and implementation of AI brought the need for policies and legal frameworks all around the globe. In this capacity USA, EU and China claimed the leader position, be it verbally or by action, their efforts setting them, one by one, as global leaders in research, development, implementation, use and AI governance in general. Each one has a different tone regarding governance and competition, publicly recognized or just assumed. Different authors note that this leadership race influences not only development and innovation, but also policy making around the globe, with an attentive focus on security matters (Clegg, 2024; Bhuiyan, 2024; China Aerospace Studies Institute, 2023).

The USA adopted a practical approach to AI policies between 2024 and 2025, focused on inter-organizational cooperation for the advancement of the USA. In October 2024 the White House adopted a document[1] through which public institutions were directed to establish policies regarding AI implementation and use, with the aim of strengthening governance mechanisms and safeguarding all of the technological developments from various external threats. The document anchored policy making in democratic values and cooperative principles, pragmatically setting a balance between innovation and resilience (Durland and Siegmann, 2024). In November 2024 *Meta* announced that

[1] Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence.

national security agencies of the USA would be granted access to the open-source version of its *Llama* LLM, further reinforcing the tone set by the memorandum in October 2024. Meta's justification revolved around adherence to democratic principles of ensuring transparency and accountability, in the greater interest of the general public, by sustaining national security (Bhuiyan, 2024; Clegg, 2024). July 2025 brought the current administration's view over AI governance, with the adoption of a new document called *Winning the Race – America's Action Plan*. Starting with the title, the entire content of the document reflects that USA's final goal is maintain global leadership over AI in general. This document sets a very clear path of AI experimentation and learning through practice, in line with principles and values specific to democracies (The White House, 2025). A complementary perspective is brought by Walker (2025), who affirmed that USA has to prioritize AI governance on three coordinates: 1) investments in hardware and software infrastructure, 2) integration of AI in defence and in intelligence domains and 3) strategic coordination of state investments in order to ensure leadership over China. This vision further reflects a pragmatic orientation, in line with recent governmental and presidential initiatives. All of these facts state clearly that USA is on a trajectory of aligning principles and values with pragmatism, ensuring a fluid AI governance policy making process, as long as the results provide global strategic advantages for the USA.

In contrast with USA's practical orientation, the EU has methodically advanced a policy and law driven approach to AI governance. The peak of this fact is the adoption of EU AI Act, the biggest and most comprehensive legal framework designed so far, which regulates AI development, implementation and use across member states (Desmarais, 2025). This act reflects EU's philosophy of governance, that of where innovation must be infused with certainty, responsibility, transparency and, above all, respect and protection of fundamental rights. In February 2025, at the *Paris AI Action Summit*, the Commission President stated that EU's advantage lies in combining cooperation between member states with open and common principles and values, all of which provide a framework that is not a general constraint, but a driver of responsible competition and safe innovation (von der Leyen, 2025). Desmarais (2025) states that a coalition of about 20 companies

reserved 150 billion euros for building an EU specific AI ecosystem, in collaboration with the EU Commission and under regulatory frameworks that combine advancements with oversight. In this matter, EU has a combined agenda, wanting to create trustworthy datasets, central and cross-members governance mechanisms, aligning AI policies with EU's fundamental principles of human-centricity. EU's AI leadership model is about adopting rules and norms, sacrificing rapid experimentation and deployment for ensuring individual, collective, state and union security and global trust.

China followed a different AI policy trajectory, further highlighting the contrasts in the global AI governance landscape. The document *Interim Measures for the Management and Generative AI Services*, emitted in July 2023, established strict AI related requirements that stretch from content moderation to security related reviews and interventions (China Aerospace Studies Institute, 2023). The Chinese approach is characterized by state control and oversight exercised through an extensive regulatory framework, public and not public. China doesn't see AI just as a means and a goal towards global leadership, it sees AI as a tool designed for governmental and social use, in accordance with national priorities. The regulatory framework aims to provide social stability and, above all, national security. Of course, the Chinese way is one of pursuing great economic and industrial achievements and in this case, AI is being treated as a catalyst of achieving global supremacy (Zhu, 2025; Lee, 2025). The Chinese model uses regulations both as instruments of internal control and as a platform of pushing international leadership and influence further. Considering this, we could say that the Chinese way is that of state driven over regulation, where every step in AI development has to be of value to the country and has to be subordinated to national interests. This development is always under the close oversight of authorities, AI providers being obliged to serve national interests first, aligning innovation and deployment with the governmental views and goals.

We called these major powers AI architects because they design AI's advancement in the world. These three major actors – USA, EU, and China – ground their strategies in different ways and approaches:

- USA sets principles and values aligned with democracy while advancing AI through practice, experimentation and public-private cooperation, all while seeking global leadership, which we call *the practical social approach to AI*.
- The EU treats AI governance in line with laws and policies, infusing AI with a normative framework that prioritizes compliance with fundamental rights; which we call *the practical normative approach to AI*.
- China adopts a state-first policy, prioritizing oversight over AI providers and users, all in the name of national interests, for economic and strategic supremacy; which we call *the practical over-regulated approach to AI*.

For intelligence agencies and for national security communities, these differences are not only words or mere theories. They are the reality in which AI tools are shaped and made available both in the benefit of society and for doing harm. Understanding regulatory frameworks and global views on AI is essential in navigating across different logics, used both by allies and by adversaries. In this regard, intelligence agencies might be able to build resilience through emulation of each approach, in order to sustain cooperation and to be prepared for adversarial usage of AI. One episode of great importance towards illustrating all of the above was generated by the deployment of a new app, called *DeepSeek*, which debuted in 2025 and took over the world rapidly. This fact alone exemplified how quickly a technological innovation can evolve into a real test of institutional resilience at a global scale.

DeepSeek: a global stress test

The emergence of the Chinese made *DeepSeek* Large Language Model (LLM) in late 2024 and early 2025 crystallized many of the dynamics between development and regulation into a single, highly visible episode, representing a practical manifestation of the accelerated development and adoption of AI capabilities. In early 2025, it became one of the first global scale tests of how different governments and different intelligence communities respond when new AI models spread faster than organizations can adapt. *DeepSeek* serves as a case study of institutional resilience in front of rapid innovation and slow public policy

adaptation. It was reported that by 13 February 2025, *DeepSeek* was the most downloaded application globally, available in approximately 156 states, with around 22.15 million daily active users and approximately 33.7 million monthly active users in January 2025. Half of those users were based in China, India, and Indonesia (Backlinko, 2025). The speed and the scale of adoption raised national security concerns, especially around data handling in general and personal data in particular. Different governments responded in different ways, for example: Italy's data protection agency suspended personal data processing for Italian citizens; Australia banned the app from all government cell phones claiming national security risks; Taiwan imposed similar restrictions, banning *DeepSeek* altogether, concerned about risks to their national security. Other countries, such as Belgium, The Netherlands, South Korea and the state of Texas opened investigations into how the Chinese made LLM manages data and interactions (Canales, 2025; del Rosario, 2025; Smalley, 2025; Sterling, 2025; The Brussels Times with Belga, 2025; Data General, 2025). A survey conducted under Euractiv (2025) showed that Cyprus, Czech Republic, Estonia, Hungary, Lithuania, Malta, Romania and Sweden reported no registered complains, while Austria, Bulgaria, Denmark, Finland, Latvia, Portugal, Slovakia and Slovenia did not respond to the survey. All of the other European states either took some measures or started investigations through their legitimate institutions.

Beyond the multiple ways in which states responded to *DeepSeek*, the debate around this app converges on national security implications. Different authors (Canales, 2025; Booth, Krupa, and Giuffrida, 2025) note that suspicions arise from the Chinese way of collecting and processing information which pose serious concerns if personal data and strategic data is involved. As plausibly presumed, the privacy and individual data protection issues are more present in the European discourse, while other political regimes treat things differently, with bans and limitations that have the role to prevent and protect. As we sweep over the literature, we see variations in the global public positions regarding *DeepSeek*, spanning from personal and general data protection to national security concerns. In both cases risks and vulnerabilities can rapidly become active threats which intelligence services and police agencies have to deal with. Starting from those reasons alone, intelligent

technologies have to be treated seriously, not only as consumer technologies, but also as potential vectors of vulnerabilities, risks and threats posed both to individual, collective and national security.

The literature indicates several types of specific vulnerabilities. These include the possibility of losing human control over intelligent technology and the risk of AI making undesirable autonomous decisions (Galliot and Scholz, 2020; Rowe, 2022; Zhou, 2024). Other risks are related to uncontrolled data collection and poor data management, which can lead to: compromised confidentiality, data alteration, and malicious use of data (Roberson, și alții, 2022; Klaus, 2024). The literature also contains numerous references to the lack of transparency of algorithms and the possibility that AI may adopt and reproduce human biases, leading to discrimination and solutions that are disproportionate to the requests (Michel, 2023; Bode and Bhila, 2024). Zhou (2024) also mentions the risk of escalating military conflicts against the backdrop of armament with intelligent technology.

DeepSeek's fast adoption amidst reasonable questions regarding personal and collective security provides at least three valuable lessons for debate in and around intelligence services:

1. the operational landscape is both national and transnational. AI apps grow and spread fast, while the organizational response can and usually is slower. Getting ready to respond to the unknown is essential and remains a constant of intelligence work. This alone is a sufficient argument for fast strategic debates that have to lead to harmonised tactical and operational responses;
2. the most acute and present risk revolves around data management, data security and dependencies that support the collection and the administration of huge data amounts. This alone brings concerns regarding potential new threats and national security risks revolving around all that is placed under the AI umbrella;
3. for adversaries, legal action and political decided bans might be an indicator of organizational readiness. Intelligence agencies might have to assess what effects would public declarations

and normative actions produce both on their own organizations and on the adversaries. The debate, in this matter, is about how public action can help or slow down the efforts of ensuring national security.

Beyond its controversies, the *DeepSeek* case highlights the strategic implications of AI on national security and for intelligence agencies. It demonstrates that vulnerabilities and risks can also emerge from rapid and uncontrolled diffusion of technology across various jurisdictions. For intelligence services, *DeepSeek* represents an important turning point, showing how various transnational approaches by different state actors are shaping a new operational landscape. In this new operational landscape, debates on global technological advances and global official public positions are mixed with new operational challenges in creating and securing national security.

AI and operational risks in intelligence

Just as *DeepSeek* was treated by some countries as a potential risk to national security, when viewing AI as a whole from a national security perspective, it is imperative to see that in addition to capabilities and opportunities, AI also brings risks. Intelligence agencies have to adapt and learn how to manage both of these two different sides of AI. Aside from pure risks, various authors (Walker, 2025; Bendett, 2024; Bond, 2024) have warned that AI could become a risk multiplier, especially in domains where automation, speed and scale can grant great advantages. The best example to this date is that of generative models that are being used widely for large-scale influence operations and disinformation. Thus, national security adversaries gain the ability to produce rapid, diverse and well-tailored narratives, supported by convincing photos and videos. AI also has the potential to lower costs and to offer precision and speed in support of malicious cyber operations (Walker, 2025). Amongst all of these, the current geopolitical situation generates great interest in infusing military tools with AI, directly affecting the way intelligent technology develops (Bond, 2024; Bendett, 2024). Bendett (2024) claims that even small progresses made in enhancing military capabilities with AI can shift tactical and operational balances, suggesting that the modern battlefield might see great disproportions

in relation with what the military expects. Considering all of these situations we might have to see AI not just a simple tool, but as a real catalyst of wide societal and historical change.

For intelligence agencies, all of the above create a very urgent need to become resilient before malicious actors can gain any kind of advantage. Despite all identified risks, it appears that for now, with the exception of disinformation and influence campaigns, adversaries have not fully exploited AI for offensive actions. Walker (2025) suggests that national security agencies still have a strategic advantage and can gain the upper hand, particularly in collection, detection and response. However, the author suggests that this period of opportunity is probably coming to an end soon. As the industry formed around AI develops more advanced hardware and more sophisticated software, more powerful and diverse models will appear, with diverse applications. Eventually, these models will spread and it is a matter of time until they will start being used for harm. Intelligence must act proactively, focusing greatly on monitoring how adversaries think, direct, innovate, implement and use AI. This is probably easier said than done, as the effort must be conjoined with a strong support from public policy makers. If we note the fact that intelligence organizations have to follow laws and ethical codes while some adversaries have no such limitations, the urgency for dialogue and for creating supporting legal frameworks becomes even greater.

The complexity of operational risks derivate from the bivalent way of using AI. Systems that are designed for benign use can become malicious in hands of malicious actors. This bivalence complicates the task of intelligence agencies, as they not only need technical expertise and legal frameworks, but a profound support from targeted research as well. Research in this field should be able to provide extensive contextual knowledge of how allies and adversaries see, develop, adapt, implement and use intelligent technology. The fact that AI can bring both opportunities and vulnerabilities creates a paradox that has to be carefully managed so that the adoption of AI at all levels of society does not produce more harm than good. Intelligence agencies must be ahead in this game and have to produce strategies that ensure resilience in providing and maintaining national security.

Organizational change and data management in intelligence

Another aspect of great importance for intelligence agencies comes from within. While the operational risks posed by AI are related to external influence and the specific nature of national security information, organizational change and adaptation are related to the influence of AI implementation in intelligence organizations. This is another perspective related to the interaction between AI and intelligence in our effort to investigate change at the level of intelligence agencies.

While looking at the private sector, Davenport and Bean (2025) documented that the year 2024 saw a doubling of organizations that made a priority out of data governance. The reality of data driven decision making is now being automatized and promises in this field might increase AI financing and adoption. While the 2024 data showed a doubling of organizations reporting data-driven culture, the 2025 survey results – which reflect responses at the time of study – suggest some regression or stagnation, with only 37% of respondents claiming to work in a data and AI driven organizations. The same moment in 2025 showed that the momentum of adopting data governance policies has slowed, with only 33% of all respondent organizations stating that they would develop data governance strategies. An interesting fact is that 92% of the questioned organizations affirmed that obstacles to full adoption and integration of AI reside in cultural views and management of change barriers. Another study conducted by McKinsey (2025) confirms the trend observed by Davenport and Bean, according to which organizations are becoming increasingly open to adopting AI, with some even becoming dependent on AI in certain internal processes. The study revealed that more than three-quarters of respondents say that their organizations already use AI solutions in at least one process. Among these processes, McKinsey (2025) highlights the automation of certain tasks, data analysis, and decision support. At the same time, the management levels of organizations are seeking to establish internal policies to ensure AI governance. The issues that AI brings to organizations are related to security, privacy, and transparency. McKinsey's (2025) conclusions argue that the success of AI integration depends both on technological innovation and on adapting the

organizational culture in terms of taking responsibility and adopting clear internal policies related to AI. We can clearly see that even though technology can rapidly advance, it is of no use if institutions that implement it are not ready for that. Without being ready, organizations will probably misuse or underutilize sophisticated tech capabilities. The problems of organizational culture and management of change are more acute in intelligence agencies, which usually operate within strict legal limits and with secrecy. This alone can make agencies more conservative. Implementation of AI will probably pose challenges in changing tools, methods, workflows, ways of treating and operating with data, all under adapted strategies and policies. As Davenport and Bean (2025) note, organizational transformations need sustained investment in human capital and in management transformation. The authors talk about cultivating trust, responsibility and adaptability, being aware of the fact that organizational cultures change at a slow pace. Intelligence organizations cannot always have the luxury of changing at a slow pace, the security landscape through which they have to navigate generating the need of fast and precise action. Therefore, intelligence agencies have to find a balance between creating resilience in front of new risks and introducing new technologies in their own ranks.

Another key issue regarding AI adoption in intelligence for national security is related to data. Roose (2024) showed that availability of high-quality data for AI training is becoming more and scarcer. Models need to continuously train; therefore, new data has to be gathered or crated. For the data to become high-quality, it needs to be cleaned, curated and structured, otherwise it could infect models with factual mistakes, biases, wrong connections and with all the consequences that this entails. According to Davenport and Bean (2025), in 2025 organizations started to realize that being competitive is not only about buying or developing the best AI models, but in data governance and data security. Intelligence services already practice collection, cleaning, structuring, verifying and analysis of data, producing high-quality information. For AI to bring scale, speed, accuracy and reliability, intelligence agencies need to gain new professional skills and orient themselves towards interdisciplinary collaboration; this fact alone

would probably be one major driver of serious cultural changes within organizations.

Organizational change will probably be a result of AI implementation and integration in various work environments. Without data governance and data security, management support and adaptive, open cultures, intelligence agencies risk becoming slow and inefficient in front of technical advancements of both their allies and their adversaries. As different authors note, success is not only about gaining cutting-edge hardware and software, but in transforming the way organizations approach AI regarding accountability, responsibility and ethical data governance (Davenport and Bean, 2025; Domanska, 2025; Walker, 2025). For intelligence agencies alone this means that their future successful missions would surely depend on internal cultural updates and normative reforms.

Conclusions

The accelerated creation and evolution of AI models between 2023 and 2025 has demonstrated that progress has the potential of not being dependent on specific industries any more. Everyone, with little or no training at all, can now generate images, videos, music and can even design interactive environments such as games and applications. Malign use of generative models has now become the main driver for disinformation, influence, control and manipulation. For intelligence agencies, this acceleration of evolving and rapid implementation of AI poses great challenges, as collection and analysis of national security relevant data now requires a new approach and a new mentality within the intelligence field of work.

At a global scale, from the perspective of policy architects and frameworks, the global race is led by three major actors, providing three distinct models. USA anchors AI development in democratic values while pursuing global leadership. This creates the need for private-public cooperation, practical lessons and great strategic investments, leading to a real *social practice* regarding AI. The EU approach is constructed around legal frameworks and specific regulations, seeing the norm as the fundamental base for trust in AI development. This leads to a *normative*

practice. China, on the other hand, believes that state driven regulation and implication is the way, prioritizing national interest in pursue of global leadership. Their ambition of gaining geopolitical supremacy and their way of over-implicating public institutions in everything creates an *over-regulated practice*, in which AI development has to have the first and ultimate goal of sustaining national interests.

The *DeepSeek* moment taught the world that a well promoted new application can take over the world with an unseen rapidity. With this kind of challenges, states are usually slow in response, as national action can only be taken after rigorous assessments and strategic analysis, a very important part of it being usually carried by intelligence communities. The key lesson here is that AI models can become matters of concern for national security, not only because new technological functionalities, but because of their potential security consequences.

Just as *DeepSeek* exemplified, from an operational perspective, AI creates a clear path for new vulnerabilities, risks and threats that intelligence have to take account of. Various authors warned about AI's potential to enhance cybercrime, to conduct disinformation and influence campaigns, to shift battlefield balances, to manipulate and control. Even though adversaries have not yet fully exploited all of AI's possibilities, the rhythm of accelerated innovation and the wide availability of models creates the need for intelligence services to anticipate and be prepared for malign use of AI as well as to develop means and methods of reaction.

For intelligence organizations to fully benefit from AI, they would have to be ready and adapt to cultural changes, while finding the best ways of assuring data governance. As the studies cited in this article have shown, public and private institutions attempted to create this type of change, only to slow down for the moment. Knowing that Intelligence agencies are slower in cultural change, both strategic management and operational layer have to be aware and acknowledge that AI governance has to be quickly assessed and implemented, so the risk of misutilization or underutilization of intelligent technology remains low.

Considering all of the above, we can come to the conclusion that AI development and deployment, global regulatory actions and organizational challenges brought by AI brought altogether pose a significant challenge for intelligence agencies. Their slower way of

adapting to cultural changes while still having to provide foresight, profound and clear knowledge of reality and rapid response mechanisms pose a problem. The mission of assuring national security in the age of AI is as hard as it gets for intelligence agencies because of different and varied currents and influences that arrive from different points. Agencies have to: adapt to new intelligent technology, finding benefits and assessing threats; navigate through various policies, that govern their own activity and that govern their adversaries' activities; be ready to respond to very rapid deployment and adoption of AI models in various domains; adapt and overcome their own inside difficulties regarding AI-brought change in organizational culture; be ready to learn how to use AI effectively to enhance their methods of assuring national security. Intelligence has to find ways of adapting from within while being ready for imposed changes from outside of their professional world. Integrating, using and understanding AI effectively has to be subordinated to the ultimate goal of assuring national security.

While the global race regarding AI supremacy brings huge investments and creates rapid innovation and implementation, it also raises one fundamental question: *how should we develop and use AI for the benefit of humanity and not against our collective interests and, above all, against our collective security?* Considering AI's potential of reshaping every aspect of social life as we know it, we should collectively try to be more cautious and more in control of our needs and wants, so that AI becomes one of our greatest instruments so far, rather than one of our greatest failures.

References:

1. Backlinko. (2024). *DeepSeek AI Usage Stats.* https://backlinko.com/deepseek-stats

2. Bendett, S. (2024). *The Role of AI in Russia's Confrontation with the West.* Center for a New American Security. https://www.cnas.org/publications/reports/the-role-of-ai-in-russias-confrontation-with-the-west

3. Bhuiyan, J. (2024). "Meta to let US national security agencies and defense contractors use Llama AI." *The Guardian*. https://www.theguardian.com/

technology/2024/nov/05/meta-allows-national-security-defense-contractors-use-llama-ai

4. Bode, I., and Bhila, I. (2024). "The problem of algorithmic bias in AI-based military decision support systems." *Red Cross – Humanitarian Law and Policy*. https://blogs.icrc.org/law-and-policy/2024/09/03/the-problem-of-algorithmic-bias-in-ai-based-military-decision-support-systems/

5. Bond, S. (2024). *How Russia is using artificial intelligence in its propaganda operations.* https://www.npr.org/2024/06/25/nx-s1-5019381/how-russia-is-using-artificial-intelligence-in-its-propaganda-operations

6. Booth, R., Krupa, J., and Giuffrida, A. (2025). "DeepSeek blocked from some app stores in Italy amid questions on data use." *The Guardian*. https://www.theguardian.com/technology/2025/jan/29/deepseek-blocked-some-app-stores-italy-questions-data-use

7. Canales, S. B. (2025). "DeepSeek banned from Australian government devices amid national security concerns." *The Guardian*. https://www.theguardian.com/technology/2025/feb/04/deepseek-banned-from-australian-government-devices-over-national-security-concerns

8. China Aerospace Studies Institute. (2023). *Interim Measures for the Management of Generative Artificial Intelligence Services*. https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2023-08-07%20ITOW%20Interim%20Measures%20for%20the%20Management%20of%20Generative%20Artificial%20Intelligence%20Services.pdf?utm_source=chatgpt.com

9. Clegg, N. (2024). *Open Source AI Can Help America Lead in AI and Strengthen Global Security.* https://about.fb.com/news/2024/11/open-source-ai-america-global-security/

10. Data General. (2025). *South Korea: PIPC announces investigation into DeepSeek.* https://www.dataguidance.com/node/641139

11. Davenport, T., and Bean, R. (2025). *Five trends in AI and Data Science for 2025.* https://sloanreview.mit.edu/article/five-trends-in-ai-and-data-science-for-2025/

12. del Rosario, S. (2025). "DeepSeek faces federal investigation over how it got its AI chips: Report." *Straight Arrow News*. https://san.com/cc/deepseek-faces-federal-investigation-over-how-it-got-its-ai-chips-report/

13. Desmarais, A. (2025). *Here's what has been announced at the AI Action Summit.* EuroNews. https://www.euronews.com/next/2025/02/11/heres-what-has-been-announced-at-the-ai-action-summit

14. Domanska, O. (2025). "Why more businesses are hiring Chief AI Officer." *Avenga*. https://www.avenga.com/magazine/chief-ai-officers-role-decoded/

15. Durland, H., and Siegmann, E. (2024). "The 2024 National Security Memorandum on AI: A Timeline and Index of Responsibilities." *Georgetown Security Studies Review*. https://georgetownsecuritystudiesreview.org/2024/11/04/the-2024-national-security-memorandum-on-ai-a-timeline-and-index-of-responsibilities/

16. Galliot, J., and Scholz, J. (2020). "The Case for Ethical AI in the Military." *The Oxford Handbook of Ethics of AI The Oxford Handbook of Ethics of AI*.

17. Klaus, M. (2024). "Transcending weapon systems: the ethical challenges of AI in military decision support systems." *Red Cross – Humanitarian Law and Policy*. https://blogs.icrc.org/law-and-policy/2024/09/24/transcending-weapon-systems-the-ethical-challenges-of-ai-in-military-decision-support-systems/

18. Lee, C. (2025). "Russia turns to China to step up AI race against US." *VOA News*. https://www.voanews.com/a/russia-turns-to-china-to-step-up-ai-race-against-us/7931829.html

19. McKinsey and Company. (2025). *The state of AI: How organizations are rewiring to capture value.* https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai?utm_source=chatgpt.com

20. Michel, A. H. (2023). "Inside the messy ethics of making war with machines." *MIT Technology Review*. https://www.technologyreview.com/2023/08/16/1077386/war-machines/

21. Moreau, C. (2025). "DeepSeek making a splash with EU data protection bodies." *EURACTIV.* https://www.euractiv.com/section/tech/news/deepseek-making-a-splash-with-eu-data-protection-bodies/

22. O'Donnel, J., Heaven, W. D., and Heikkilä, M. (2025). "What's next for AI in 2025." *MIT Technology Review*. https://www.technologyreview.com/2025/01/08/1109188/whats-next-for-ai-in-2025/

23. Roberson, T., Bornstein, S., Liivoja, R., Ng, S., Scholz, J., and Devitt, K. (2022). "A method for ethical AI in defence: A case study on developing trustworthy autonomous systems." *Journal of Responsible Technology,* vol. 11.

24. Roose, K. (2024, Iulie). "The Data That Powers A.I. Is Disappearing Fast." *New York Times.* https://www.nytimes.com/2024/07/19/technology/ai-data-restrictions.html

25. Rowe, N. (2022). "The comparative ethics of artificial-intelligence methods for military applications." *Frontiers in Big Data vol. 5*.

26. Smalley, S. (2025). "Texas investigating DeepSeek for violating data privacy law." *The Record.* https://therecord.media/texas-investigating-deepseek-privacy

27. Sterling, T. (2025). "Dutch privacy watchdog to launch investigation into China's DeepSeek AI." *Reuters*. https://www.reuters.com/technology/

artificial-intelligence/dutch-privacy-watchdog-launch-investigation-into-chinas-deepseek-ai-2025-01-31/

28. The Brussels Times with Belga. (2025, Ianuarie). "Investigation opened into possible privacy violations by DeepSeek." *The Business Times*. https://www.brusselstimes.com/1419622/investigation-opened-into-possible-privacy-violations-by-deepseek

29. The White House. (2025). *America's AI Action Plan*. https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf

30. von der Leyen, U. (2025). "Speech by President von der Leyen at the Artificial Intelligence Action Summit." *European Comission Press Corner*. European Comission. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_25_471

31. Walker, K. (2025). *AI and the future of national security.* Google Threat Intelligence Group. https://blog.google/technology/safety-security/ai-and-the-future-of-national-security/

32. Zhou, W. (2024). "Artificial intelligence in military decision-making: supporting humans, not replacing them." *Red Cross – Humanitarian Law and Policy*. https://blogs.icrc.org/law-and-policy/2024/08/29/artificial-intelligence-in-military-decision-making-supporting-humans-not-replacing-them/

33. Zhu, S. (2025, Ianuarie). *Transforming industries with AI: Lessons from China's journey.* World Economic Forum. https://www.weforum.org/stories/2025/01/transforming-industries-with-ai-lessons-from-china/

SECURITY IN THE 21ST CENTURY

EXTRAPOLATING SECURITY: WHEN EVERYTHING IS SECURITY, NOTHING IS SECURITY!

Ioana LEUCEA*

Abstract:

The usage of the concepts and words less for their denotative meaning and more for their connotative ones may seem unproblematic at a first glance. Yet the constant usage of language not for the primary significance of words may spread a lot of confusion even within the domain of strategic thinking. While scholars struggle to define and to clarify the concepts they use in order to develop a school of thought to prevent war and conflicts or the emergence of dangerous social phenomena, it seems that at the socio-political level the clarity is lost as the elusive interpretations proliferate.

The conventional wisdom developed after the end of the Cold War envisaged the concept of security in terms of expanding and deepening its meaning. The Copenhagen school advocated for different social domains to be included within the concepts of national, regional or global security, leaving the impression that the security risks are ubiquitous, that no social arena was to be left outside the security compass: be that culture, politics, or education. Every communication act would be monitored for the possibility of containing the seeds of evil, name them propaganda, disinformation, misinformation or fake-news. Film productions or literature are included here as well. Expressions like "cognitive warfare" or "hybrid warfare" have produced more confusion as it is presumed that there are no real peace periods but only war time preparation and that the social reality cannot not be defined in terms of real cooperation. For instance, assuming that specific issues of lesser importance should be included in the category of national security issues, in terms of comprehensive security, the door to intervention opens: the security services are allowed to intervene within the private or social spheres while these are supposed to be free of surveillance or monitoring.

Additionally, the analysis we propose intends to focus on the importance of finding the proper language for organizing the social space when speaking about security matters, as the management of national security depends a lot on the conceptual toolbox.

* Associate professor PhD, "Mihai Viteazul" National Intelligence Academy, Bucharest, Romania; email: leucea.ioana@animv.eu. Disclaimer: the material is a reflection of the authors' opinions and beliefs, and does not represent the opinions, policies or the views of the Romanian Intelligence Service or the National Intelligence Academy "Mihai Viteazul".

The article upholds the idea that by extrapolating the meaning of security, the words and concepts associated with it generate but confusion, which leads to poor management and organizational errors.

Keywords: *security; concepts; language; culture; cognitive warfare.*

Introduction

The concept of security has gained an almost ubiquitous popularity. It seems that the world has become such a dangerous arena that people must strive every second to survive. The extrapolation of the significance of the term "security", which initially was used within the domain of military defence and war strategies, has lost its core definition and nowadays it has been transferred to almost all social spheres/ domains. We are now speaking about social security, food security, human security, state security, political security, economic security, financial security, medical security, educational security, communication security, and energetic security and so on. The same thing happens when we speak about threats or hybrid threats. The threat may refer to any type of risks, be they minor or catastrophic. There is no doubt that there are real problems, but the concept has become tautological and redundant as long as any political domain implies a security rationality.

As in the case of the broad definition of human security paradigm, the concept loses its contours and its possibilities to configure a security agenda. In this context, we may assume as well that a culture of fear has become prevalent. If fear becomes part of society's daily life, this gives birth to a culture of fear (Mölder and Shiraev, 2021).

Extrapolating the connotative meanings of concepts

The usage of the concepts and words less for their denotative meaning and more for their connotative ones may seem unproblematic at a first glance. Yet the constant usage of language not for the primary significance of words may spread a lot of confusion even within the domain of strategic thinking. While scholars struggle to define and to clarify the concepts they use in order to develop a school of thought to prevent war and conflicts or the emergence of dangerous social phenomena, it seems that at the socio-political level the clarity is lost as

the elusive interpretations proliferate. Hannah Arendt (1968) noticed as well that key words selected and used within the socio-political discourse, such as liberty, justice, responsibility, virtue, power, glory lost their original spirit by their usage uprooted from the phenomenological reality. Equally, the same thing happens when speaking about the corrupt meaning of the words security, strategy and (hybrid) threats.

In my opinion, the subject of extrapolating the connotative meanings of the security concept refers to the issue of an abusive and improper way to utilize it, which, as in the case of the concept of strategy, has almost lost its meaning. (Hughes, 2014). The human security paradigm, developed within the post-Cold War period, expanded indefinitely the threats and risks to human life, leading to an almost never-ending list of security problems, be they related to poverty, underdevelopment, medical problems, societal violence, and political problems (Leucea, 2012). There is no doubt that the risks are real, yet the questions and the dilemmas are related to prioritizing and organizing the security agenda. As the security agenda has progressively expanded from the paradigm of securing the state towards human security, concepts like responsibility to protect, human rights, good governance, humanitarian interventions have been brought forefront and the need for rethinking the security concept indicates in fact a crisis of global organization and governance. In terms of ontological security, the dilemma between securing the state and securing the people involves a definition of international society or the answer related to reaching the consent at the global level related to answering the question as to who are the legitimate political actors on the global stage. Should or should not certain actors be recognized as legitimate political actors on the global scene? Who deserves to be protected? People or states?

When discussing the connotative meanings of strategy concept, Strachan (2005, p. 34) noticed the same: "The word 'strategy' has acquired a universality which has robbed it of meaning, and left it only with banalities." (Strachan, 2005, p. 34) Moreover, Hughes (2014, p. 50) highlight that the term strategy used by governments to describe the diverse politics implemented during peacetime periods and less by armies during war times have gained popularity, yet the conceptual clarity was lost. Carl von Clausewitz (1982) correlated the word strategy with war and Antoine Henri Jomini (1992) considered that "strategy" is

the key in winning the war. Etymologically, the meaning of strategy derives from the Greek word *strategos* having the significance of a military rank, that of a general (Hughes, 2014, p. 50).

Similarly, with the deepening and the widening of the concept of security as the Copenhagen school understands it, the same happened with concept of strategy, the domains that integrated the term have been diversified and amplified. It has almost become a *cliché* within the domain of strategic studies to affirm that we may speak about a paradigmatic change in understanding and conceptualizing strategy and that the progress has been made from a narrow interpretation of the concept to a comprehensive approach of it (Buzan, Waever and De Wilde, 1997). The newly emerged interest for themes like cognitive warfare, manipulation, propaganda, fake-news, and misinformation and so on posits the term strategy within the realm of communication, revealing an entire spectrum of instruments of communication, be they offensive or defensive.

Even the notion of war has been extrapolated to other social domains – weaponization of narratives, for instance – yet the hard meaning of war, *direct aggression executed by the armed forces of a state,* was less perceived as the main threat or risk. The idea of weaponizing discourses for attaining certain goals has also gained importance. The term weaponizing was as well correlated to ideologies or with the culture of uncertainty (Brezinsky, 2007). Similarly, in the whole society approach when speaking about the need of securitization of all domains transforms the entire society into a garrison, a military organization (Mölder and Shiraev, 2021, p. 14). As Raymond Aron (1958, p. 73) once said, the fear of war is often a tyrant's opportunity for preserving a totalitarian (as well as authoritarian) regimes.

Designing the international order: from the anarchic international society towards a cognitive anarchy

The limits of the traditional security paradigms that have structured the world in the past are no longer valid when mapping the international system today and implicitly when making a worldwide threat assessment, but the extrapolation of the security concept in almost any social domain involves the loss of its hard definitions. Therefore, we may assume that when everything is security, nothing is security and

signal that it is necessary to recover the core meaning of the security concept and its use in a proper way when mapping the international security environment.

The theoretical lenses used by the intelligence and political communities in assessing the international security environment have been configured by the traditional theories of international relations, be that classical realism, neorealism or neoclassical realism or by liberal and neoliberal paradigms. The traditional perspectives assumed a positivist ontology of the international society which was composed of a number of states functioning on the basis of certain understandings and rules of behaviour. The evolution of the global society has determined the specialists to reflect upon the traditional analytical frameworks of conceiving security. As the new digital/virtual realities imply even the modification of the human psyche, specialists created the term of "cyber-psychology" in order to highlight the deep influences the digital media has on people's mind and behaviour. Moreover, the fact that the communication environment has become the new battleground, the antechamber of war, brings to the foreground some elements having deep historical roots: a constant evolution of the conflicts and wars translated within the organizational field of the international society and its historical transformational processes. The configuration of the international order becomes a political goal as the construction of international society involves at least a general consensus of the great powers on how the world should look like or be composed of. Throughout history, the agreement of great powers on certain international principles was paramount for peace and stability (Clark, 2007).

The evolution of the international systems has been correlated with war and conflicts. The limits of the security dilemma the realist International Relations school of thought revealed, aggravated by the thinking provided by the offensive realism paradigm, and the prophecy of the unescapable tragedy of power politics, envisaged the counterproductive realist security paradigm when speaking about arms race, for instance, while securing the state (Mearheimer, 2010). As long as human history has demonstrated that the risk of war is enormous, securing the state by military means may become the main source of insecurity. The arms' race represents a global dynamic that endangers

the entire humanity, not only the states. The proliferation of nuclear weapons is such an example.

The constructivist approach of International Relations reveals very important ideas when discussing security issues, namely re-examines the ontological condition of the existence of society. The traditional security paradigms, realism and liberalism, assume the existence of the state, without questioning too much the societal dynamics which may modify dramatically its existence, be that war, migration (emigration or immigration), pandemics or identitarian phenomena. The culture, the ideas and the values people share, as constructivism upholds, have become nowadays the critical infrastructure in securing the state. Moreover, the nexus between education and security is more relevant than ever even for securing the state. The social realities are configured by cultural infrastructure and the goal of securing the state should be mediated by the cultural and educational framework. The ontological assumption of the existence of the states on which IR realism and liberalism are based when designing security strategies overlooks the constitutive "bricks" of a state: the will of people, their identities (Leucea, 2012). As the global order has firstly a cultural foundation, revisiting the principles of the global order should involve a general agreement upon basic principles. What is a state? What is international society? Who are we/they?

The formation or the fragmentation of the states is highly dependent on the legitimation principles, if not on coercion. Who is entitled to decide upon the right of existence of certain states or people? And the right answer might be that nobody or anybody. The formation of the states depends firstly upon the political will of the people, on its recognition on the global political map, preferably by all other states. From an ontological point of view, the national sovereignty assumes valuing the cultural specificity. The constitution of the international system derives from the deep-seated social values, from the intersubjective meanings people share and it is based on the agreement shared by the global actors upon the fundamental organizing principles: the world is composed of national states or it is composed of negotiated identities (Leucea, 2022).

The realist theory of IR places the concept of the balance of power at the centre of the systemic interpretation of security. The constitution of the international society, as David Philpott (2001) discusses, relies on the intersubjective understandings related to organizing social identities and on the function of the states. The international community of humankind cannot be primarily defined by the state's frontiers. The assumed anarchic condition of the international system, the world described in terms of state – system, a number of sovereign states that act for securing their existence, represents a picture depicted as being an objective condition, but it lacks the ultimate rationality: the cognitive maps people share, the tacit constitution of the international society (Philpott, 2001).

From the personal identities towards social identities, the world organization relies on people's perception of international reality. The understanding of our place in the world involves values and personal definitions: are we free individuals or subordinates of some systems? Do we have the liberty to participate in negotiations about who we are in the world or the definition should be imposed by coercion and military force? The idea that security is indivisible, that insecurity is exported and that the security challenges have a global dimension requires as well answers related to values.

While George Orwell in his dystopian novel "1984" describes a perpetual war – "Attention! Your attention, please! A newsflash has this moment arrived from the Malabar front. Our forces in South India have won a glorious victory!" – the description must be read in terms of self-constructed, often adversarial worlds that are permanently challenging one another and making the international system extremely destabilized and vulnerable (Mölder and Shiraev, 2021, 14). Many of these competing worlds have relied on more or less totalitarian or authoritarian ideologies. Totalitarian and authoritarian regimes try to play hard with the weaknesses of liberal democracies, be that populism, corruption, control or strategic imagination: "The ability to produce effective strategic imagination becomes more and more apparent these days. Strategic advantage can be obtained by changing the rules or deliberately creating turbulence" (Stan Glaser, 1994, 31).

Failure of imagination leads to serious security failures, as Zbigniew Brzezinski (2007) once argued that the culture of fear "obscures reason, intensifies emotions and makes it easier for demagogic politicians to mobilize the public on behalf of the policies they want to pursue." A culture of irrational responses, long-lasting uncertainty and fear causes irrational demands. Officials – being under pressure of fear and uncertainty – make policy mistakes, which further lead to irrational reactions of the people (Mölder and Shiraev, 2021).

All this translated into the language of security studies indicates the ideological warfare: "It is a clash of fundamental ideas or principles referring to economy, government, politics, lifestyle, or life in general. For example, social conflict ideologies, like Marxism, focus on capitalism and inequality. Neo-Marxists often focus on race and colonialism. Political ideologies, like conservatism and liberalism, also make judgment calls about the structure and functioning of economic, social, and political forces. Nationalism calls attention to nation – centred models of development – American, French, Russian, and Chinese, among others, strongly emphasizing the idea of their exceptionalism. Civilizational ideologies are rooted in deep-seated cultural principles, such as Western, Eurasian, Muslim, Hindu, and Confucian, among others. These are, of course, just the most prominent ideological clashes the modern world is experiencing." (Mölder and Shiraev 2021, 17)

If the entire world is experiencing a constant state of fear, anxiety, conflict, we may presume that by extrapolating the security concept to every social domain the result would be very much the same. When presuming the goal of targeting democratic election, the entire socio-political arena becomes a theatre of operations. Yet the aim might be creating a culture of confusion, a revised state of the nature characterized by the Hobbesian phrase "*homo homini lupus est".*

The weaponization of a nonsense: illiberal democracy

The debates about populism have been extended within the academic sphere, as the phenomenon of populism is correlated with the democratic crises and the proliferation of the hybrid regimes, namely illiberal democracies. The IR realist security paradigm would bring the best arguments for limiting the spread of democracy worldwide. If the

enemy of autocrats are the democratic rules, then the realist paradigm of IR is their best ally. In fact, the axis of autocrats tries to elude the concept of good governance which becomes the indispensable instrument to be employed when speaking about human security and human rights (Leucea and Sofonea, 2022).

Promoting illiberal values[1] by some populist leaders (e.g. Viktor Orbán, Hungarian Prime Minister, the upholder of the idea that "his illiberal democracy despises the tolerance for minorities and rejects the control and the power equilibrium," or Erdogan's rhetoric question: Who are you? We are the people!), more often than not means xenophobic discourses that exclude certain minority rights or individual rights, but in terms of power politics the goal would be to weaken the democratic world by valuing the communitarian argument, as if the individual has less rights when confronting the majorities' will.

Although there are opinions that assume the democratic character of populism, within an autocratic regime this embodies the perfect tool for gaining more power, without resorting to other democratic principles, be that the limited number of presidential mandates. If the main challenge for authoritarian regimes is to deny and reject the democratic rules, the social condition of fear, crises and war favour dictatorial and military attitudes of the leaders. If the world is in great danger, there is no place for democracy. Democracy would be subordinated to military regimes. The proclaimed twilight of democracy (Applebaum, 2020) must be perceived within the context of growing populist leaders and the seductive lure of authoritarianism. The fake-concept of illiberal democracy represents the perfect instrument in order to gain more power and control. When the number of presidential mandates in certain countries were permitted to be more than two, the concept of democracy was reinterpreted not in terms of a mechanism to

[1] The academia promoted the phrase as well, many books being written on the theme of illiberal democracy, among which: The Future of Freedom: Illiberal Democracy at Home and Abroad (2007), Towards Illiberal Democracy in Pacific Asia (1995), Democracy Denied: Identity, Civil Society, and Illiberal Democracy in Hong Kong (1999), Temptations of Power. Islamists and Illiberal Democracy in a New Middle East (2014), Illiberal Democracy in Indonesia. The Ideology of the Family-State (2015), Democratic Decline in Hungary. Law and Society in an Illiberal Democracy (2018).

prevent the centralization of power, yet as an exercise of control. By modifying the Constitutional rules and by resorting to people's will in doing that, the authoritarian leaders exploited the referendums in their favour. Stalin's quote may explain the situation: "it's not the people who vote that count, it`s the people who count the votes."

The fact that the concept of illiberal democracy is an oxymoron, a contradiction in terms (Cornea, 2019) was not a sufficient argument for the concept not to gain popularity. By reducing democracy to the narrative "we are the people", we are the majority, and the concept of illiberal democracy was strategically launched in the global arena. The Hungarian Prime Minister, Viktor Orbán, had an important role in doing that in 2014. The same year, coincidence or not, Crimea was annexed by the Russian Federation by employing the democratic device of organizing a referendum most probably with predetermined results. The notoriety of the concept, although being a nonsense, reflects in fact the success of the authoritarian regimes' propaganda. Instead of naming the regimes' dictatorships, by using formulas like hybrid democracies, partial democracies, guided democracy, electoral authoritarian regime, void democracy and so on, the populist leaders sell the idea that they provide democratic regimes but in small portions. Moreover, Viktor Orbán (2014), upholder of the idea that "his illiberal democracy despises the tolerance for minorities and rejects the control and the power equilibrium" has made great steps towards legitimizing it.

Turkey under Recep Tayyip Erdoğan has become a case study for illiberal democracy. The populist leader has exploited the nonsense of illiberal democracy to achieve power centralization. Andrei Cornea (2019) has written that by using the phrase illiberal democracy we do a favour to those tyrants by playing within their theatre of operations. By naming their regimes democracies we bring them compliments, we make a bow in front of them. Domenico Fisichella (2007, 313) insisted on the idea that in order for a regime to be called democratic it is not enough for people to vote. For the classical liberals like Benjamin Constant, Alexis de Tocqueville or John Stuart Mill, the danger of the tyranny of majority was obvious (Cornea, 2019). The emblematic statement of the Turkish president, "We are the people! So, who are you?", represents the core idea for populism, yet, as Karl Popper revealed, the emergence of

democracy as a political reality and as a philosophic term was not related to people's sovereignty, but it was the name given to a Constitution that is the opposite of a dictatorship (Popper, 1994, 157).

A defining feature of democracy, the majority rule, which often leads to populism should play a secondary role. The theory of democracy, understood as preventing the abuses of power, supports mechanisms such as limited mandates, separation of powers, the rule of law, multiparty system, periodical organization of elections etc., mechanisms that aim to protect the individual and the minority rights, to avoid dictatorship, be it the dictatorship of the parliament, of the masses or of other political groups. Therefore, we question the possibilities of overcoming the contradicting meanings of democracy, its legitimation – through the exclusive vote of majority – of certain illiberal policies, especially those included in the broader spectrum of xenophobia and discrimination by politicizing identities.

A critical reflection on the concept of democracy in relation with the values a society should be upheld and protected from being confiscated by political parties in their electoral fight, as sensible values like traditional family ethos or children's sexual education, subjects haunted for their high impact on society, should not be misused for partisan purposes. Organizing referendums for critical and important issues should be an instrument to fundament politics, yet not the definitive one as it could succumb as well to populism. We believe that the civil society should play an important role in the conduct of political battle by emphasizing and upholding some constitutional rules for the benefit of the whole society. The reconceptualization of national interest or of the public interest in a democratic way would be at stake as it depends deeply on theorizing democracy by emplacing the individual rights and the role of institutions within the political space. There are many voices in society that complain about the politicization of different social institutions which should be apolitical and have civil character.

Conclusions: towards an international constitution

Extrapolating the meaning of security and the expansion of its usages in almost any social sphere, be that internal or external, might indicate in fact the lack of consent in understanding international society. What is international society? How should it be configured for a more

stable security environment? In which degree the transformation of the global scene may bring more security or less security, as it seems every social arena involves a security rationale. For instance, the fight of the dictatorships against democratic rules exploits the camouflage of the fight against the American hegemony and the correlative antagonist concept: multipolarity. The autocrats can hardly reject the democratic values *per se*, yet by conflating the democratic values with the American foreign policy the fight borrows the appearance of a right, one perceived as legitimate in the field of international relations. The autocrats are not directly denying the value of human rights, but they reject US foreign policy as a supporter of the democratic system. By using nonsense concepts like illiberal democracy, the autocrats use the shiny lure to remain for decades in power. The arsenal for discretization of democracies employed by the authoritarian leaders contains as a special ingredient the presumption and the indemonstrable liaisons with the CIA. Applebaum (2025, p. 117) gives some examples in revealing the tactics. The author mentions for instance the writer Gene Sharp, who was accused of collaboration with the CIA and who published in 1994, in Bangkok, the book entitled *From Dictatorship to Democracy.*

Nowadays the authoritarian regimes in order to discredit their adversaries are claiming that the invocation of democracy, justice or the rule of law are nothing more than proofs for treason, foreign connections or external financing (Applebaum, 2025, pp. 127 and 129), assuming that there's no idealism or patriotism to explain the determination of some individuals to risk their life in the fight for freedom. The liberal order constructed after World War I replaced the balance of power system with the common security and the creation of the League of Nations. The liberal order had in centre the human rights concept: the international society was to be understood as an international society of peoples, not simply of states (Clark, 2007, p. 12).

The deep cultural structure of the international system the autocrats try to rewind is the liberal one, based on the value of individual liberty. To revolve in the mind of people that the social identity – our identity – take precedence over the individual identity reflect the deep cultural structure of the informal constitution of international society the autocrats want to change. The constitution of international society as Philpott (2001) name the concept, that the autocrats try to impose is one

composed of states, led by irremovable elites, less by people. The death in prison of Alexey Navalnii, the leader of the opposition party in the Russian Federation may represent such a victory for the elites in power. On the international arena a profound contestation of the fundamental democratic and human rights values is underway, not to question the legitimacy of the dictatorships in the name of stability. The fact that more and more people question the international society's design and organization, its core principles, its units, the fundamental bricks of the international system, may indicate that a revolution in sovereignty is underway. In this regard, Philpott (2001, 5) mentions: "The eccentricity of international revolutions, the reluctance to remember them, I further suspect, lies in the strangeness of the very idea of an international constitution." The modifications involve the cognitive map people use to interpret and perceive the world, the cultural infrastructure functioning like an international constitution and we believe that the extrapolation of security does not imply more security, but less individual liberty, a situation which favours the axis of the autocrats.

References:

1. Applebaum, A. (2020). *The Twilight of Democracy. The Seductive Lure of Authoritarianism.* Doubleday.

2. Applebaum, A. (2025). *Axa autocraților [Axis of Autocrats]*. Bucharest: Litera.

3. Aron, R. (1958). *On war: Atomic weapons and global diplomacy*. Secker and Warburg.

4. Arendt, H. (1968). *Between Past and Future: Eight Exercises in Political Thought*. New York: Viking Press.

5. Bell, Daniel, David Brown, Kanishka Jayasuriya and David Martin Jones. (1995). *Towards Illiberal Democracy in Pacific Asia*. London: St. Martin Press and Palgrave Macmillan.

6. Bourchier, David. (2015). *Illiberal Democracy in Indonesia. The Ideology of the Family-State*. London and New York: Routledge.

7. Brzezinski, Z. (2007, March 25). "Terrorized by 'War on Terror'." *The Washington Post.* https://rikcoolsaet.be/files/2007/03/brzezinski-250307.pdf.

8. Bull, H. [1977]. (2002). *The Anarchical Society. A Study of Order in World Politics*. New York: Columbia University Press.

9. Buzan, Berry, Waever, Ole and Jaap de Wilde. (1997). *Security: A New Framework of Analysis,* Lynne Rienner Publishers Inc.

10. Clark, I. (2007). *Legitimacy in International Society*. New York: Oxford University Press.

11. Clausewitz, Carl von. (1982). *Despre război [On War],* Bucharest: Military Publishing House.

12. Cornea, Andrei. (2019). "Nu există democrație iliberală" [*There is no illiberal democracy*], *Dilema veche*, no. 784, 28 February-6 March 2019, https://dilemaveche.ro/sectiune/situatiunea/articol/nu-exista-democratie-iliberala

13. Fisichella, Domenico. (2007). *Știința Politică. Probleme, concept, teorii. [Political Science. Problems, concepts, theories].* Iași: Polirom.

14. Fitzi, Gregor, Jürgen Mackert and Bryan S. Turner. (2019). *Populism and the Crisis of Democracy*, London and New York: Routledge.

15. Glaser, S. (1994). "The strategic imagination." *Management Decision*, 32(6), 31–34.

16. Hamid, Shadi. (2014). *Temptations of Power. Islamists and Illiberal Democracy in a New Middle East*. Oxford and New York: Oxford University Press.

17. Hughes, G. (2014). "Strategists and Intelligence" in Dover, Robert, Michael Goodman and Claudia Hillebrand, *Routledge Companion to Intelligence Studies*, London and New York: Routledge.

18. Jomini, Antoine-Henri. (1992). *The Art of War,* Lexington: Old Army Books.

19. Levitsky, Steven and Lucan Way. (2010). *Competitive Authoritarianism. Hybrid Regimes after the Cold War.* Cambridge, New York: Cambridge University Press.

20. Leucea, Ioana. (2012). *Constructivism și securitate umană [Constructivism and human security],* Iași: Institutul European.

21. Leucea, Ioana și Mihai Sofonea. (2022). *Schimbarea și societatea internațională [Change and international society],* București: Topform.

22. Leucea, Ioana. (2022). "Cognitive Warfare in Designing International Society (and Security Environment)", in *Redefining Community in Intercultural Context*, vol. 11, Sibiu: "Henry Coandă" Air Force Academy Publishing House.

23. Mearsheimer, Jon. (2010). *Tragedia politicii de forță [The tragedy of power politics],* Bucharest: Antet Press.

24. Mölder, Holger and Eric Shiraev. (2021). "Global Knowledge Warfare, Strategic Imagination, Uncertainty, and Fear," in Holger M., Sazonov V., Chochia A., Kerikmäe T. (eds.). *The Russian Federation in Global Knowledge Warfare. Influence Operations in Europe and Its Neighbourhood.* Springer, pp. 13-32;

25. Mudde, Cas and Rovira Kaltwasser. (2017). *Populism. A Very Short Introduction*. New York: Oxford University Press.

26. Norris, Pippa and Ronald Inglehart. (2019). *Cultural Backlash: Trump, Brexit, and the Rise of Authoritarian-Populism.* Cambridge: Cambridge University Press.

27. Orban, Viktor. (2014). "Prime Minister Viktor Orbán's Speech at the 25th Bálványos Summer Free University and Student Camp". https://www.kormany.hu/en/the-prime-minister/the-prime-minister-s-speeches/prime-minister-viktor-orban-s-speech-at-the-25th-balvanyos-summer-free-university-and-student-camp

28. Orwell, G. (1949). *1984*. New York and Scarborough: New American Library.

29. Pap, András. (2018). *Democratic Decline in Hungary. Law and Society in an Iliberal Democracy*. London and New York: Routledge.

30. Philpott, D. (2001). *Revolutions in Sovereignty. How Ideas Shaped Modern International Relations*. Princeton and Oxford: Princeton University Press.

31. Popper, Karl. (1994). *În căutarea unei lumi mai bune [In search of a better world]*. Bucharest: Humanitas.

32. Thomas, Nicholas. (1999). *Democracy Denied: Identity, Civil Society, and Illiberal Democracy in Hong Kong.* London and New York: Routledge.

33. Vukovich, Daniel. (2019). *Illiberal China. The Ideological Challenge of the People's Republic of China.* Singapore: Palgrave Macmillan.

34. Zakaria, Fareed. (2007). *The Future of Freedom. Illiberal Democracy at Home and Abroad*. New York: W. W. Norton and Company.

35. Strachan, H. (2005). *The Lost Meaning of Strategy*, Survival: Global Politics and Strategy, 47(3), 33–54.

36. Strachan, H. (2007). *Carl von Clausewitz's 'On War': A Biography*, London: Atlantic.

ASSESSING NATO'S READINESS TO RELEASE A BLACK SEA STRATEGY BASED ON DYNAMICS PRIOR TO NEGOTIATIONS FOR PEACE IN UKRAINE

Ana MOIAN*

Abstract:

Despite the importance of the Black Sea, a region characterised by acts of aggression, competition for resources, expansionism, and political instability, NATO does not have an official security strategy for it, even after witnessing three years of war in Ukraine. Developments of early 2025 make it even more unclear if the allies are able to come to common grounds regarding the instruments of power that will be used to defend this area. Based on the evolutions witnessed prior to negotiations for peace in Ukraine, this paper examines the likelihood that NATO will take this action, emphasising the contributions of its riparian states, Türkiye, Bulgaria, and Romania. Using a theoretical framework established by Dr. Harry R. Yarger for understanding strategy, but extrapolating his insights from national level to an alliance level, this paper attempts to extract the advantages, difficulties, and primary areas of focus for developing this strategy by providing an analysis of scholarly literature, official documents, and primarily perspectives from these three nations. Important conclusions include the necessity of unifying different national priorities to improve responses to Russian aggression, the need for alternative measures to assure stronger deterrence, and the necessity of strengthening regional cooperation to assist the endeavour.

Keywords*: NATO; Black Sea; strategy security; Russia.*

Introduction

The Black Sea Region includes, at first glance, the littoral states Romania, Bulgaria, Turkey, Georgia, Russia, and Ukraine. Since the 24th of February 2022 – the day that marks the start of Russia's full

* Graduate Student, "Mihai Viteazul" National Intelligence Academy. Email: finadoraboanta@gmail.com. Disclaimer: the material is a reflection of the authors' opinions and beliefs, and does not represent the opinions, policies or the views of the Romanian Intelligence Service or the National Intelligence Academy "Mihai Viteazul".

invasion of Ukraine – it has been proved again to be the front-line region for the North Atlantic Treaty Organisation's deterrence efforts against Russia's revisionism.

Three of these states – Romania, Bulgaria, and Turkey – are NATO members. The first two, despite being former communist one-party states and former satellites of the Union of Soviet Socialist Republics, are now providing an example of ascension and integration in the Euro-Atlantic system and of potential to exercise a more important role in Europe. With Russia seeking to prevent the replication of this model in former Soviet territories, the security architecture of this area becomes hard to navigate. Turkey finds itself in a position of trying to balance between NATO and Russia; Romania and Bulgaria are on a path to build their military capabilities to adapt to the level of threat in the Black Sea, and the allies are still reluctant to grant membership to Ukraine and Georgia, without prospects of their position changing too soon.

Given the apparent prolongation of conflict in the region, with the war in Ukraine continuing into 2025 and territories of Moldova and Georgia still under Russian occupation or control, it appears most likely that the Black Sea area will remain a key for pushing back Russia, at least for the European part of the alliance. Especially in times of uncertainty, a clear strategy would provide guidance on how defence and deterrence can be effectively managed in the long term and will prove common pro-activeness and anticipation capability of the allies in a changing political environment. A security strategy for this region, once established, could affirm NATO's commitment to preventing the Black Sea from becoming a "Russian lake", for example, by presenting a common set of objectives considered.

Although it might seem late or even more complicated, the allies coming together and agreeing on a strategic document is still needed in treating sovereignty challenges in the region (Atlantic Council, 2020), at least as an act of signalling deterrence through the expression of a common view on how the alliance will commit to defending this area long-term. Irrespective of the outcome of the war in Ukraine, taking into account that Russia's interest in the area will most likely never diminish, the allies will always have to choose how to defend from this potential adversary. Russia most like will still engage in the Black Sea as it is a

strategic gateway to warm water ports throughout the whole year, with Sevastopol and Novorossiysk on the route to access the Mediterranean Sea, that can secure the possibility for an extended military presence in the Middle East and not only. This is indicated by Russia modernising the Black Sea Fleet and the Southern Military District through the State Armaments Program (Hodges et al., 2022) and being now in a position of power obtained by the illegal annexation of Crimea, which allows it to use this strategic point to target all the Black Sea states by utilising the capacities built in the peninsula (DSCFC of NATO PA, 2023).

Besides the risks, threats, and vulnerabilities to the security of the littoral NATO members and their allies caused by Russia's expansionism, in the long term, considering a wider interconnected Black Sea Region that includes Moldova – indirectly connected to the Black Sea through Giurgiulești Port, Azerbaijan, and Armenia – the allies will have to take into account the implications of Iran and China as future key players that can significantly influence the dynamics in the region. Chinese expansionism is already visible in the neighbouring areas like the Caucasus, Central Asia, or even in European states.

Aim, objectives, and theoretical framework of the research

As of early 2025, NATO does not have an official strategic document regarding the security of the Black Sea region, this article aims at assessing NATO's readiness to develop it, starting from the hypothesis that a strategy is clearly needed in a region prone to crisis, in order to reflect the common choice of the allies on how to use their power to defend from threats originating here. In pursuit of this goal, the article will identify the benefits and challenges of agreeing on such a document, the implications of NATO's presence on the regional security environment, the importance of cohesion between the littoral allied states, while also trying to contribute with policy recommendations.

The research will employ a qualitative literature review, examining scholarly works, official documents, and open-sourced data. The current research available on this topic mainly consists of articles focused on the reasons NATO states in the area are incapable of coming to strong common grounds regarding some crucial aspects of foreign affairs. This paper seeks to analyse NATO's readiness to adopt a Black Sea security

strategy, by evaluating if the allies have already built some of the premises, meaning that it would be easier to translate them into a strategy. The evaluation will take into account the progress documented before the start of negotiations for peace in Ukraine.

As a theoretical framework for assessing NATO's readiness to engage in the adoption of a security strategy for this area, this paper will analyse if statements and actions, before early 2025, are strong indicators that the alliance is already able to develop a good strategy according to the criteria put together from various theories by Dr. Harry R. Yarger in "A Conceptual Foundation for a Theory of Strategy" (Bartholomees, 2006). He identifies several key premises for building a strategy:

- a strategy should be proactive, showing how to use the power available;
- the strategist must know what is to be accomplished, meaning the end-state which is desired to be achieved;
- the strategy must identify an appropriate balance among the objectives, the methods and the resources;
- political purpose, meaning the desired end-state defined by governments in policies, must dominate all strategy;
- strategy is hierarchical, meaning that it represents the views of a leader;
- strategy is comprehensive, being influenced and influencing the environment;
- strategy is developed from a thorough analysis and knowledge of the strategic environment, by highlighting all the factors that support it or could interfere with its implementation;
- risk is inherent, and the best any strategy can offer is a favourable balance against failure (Bartholomees, 2006).

These premises were turned in research questions about NATO's behaviour in the Black Sea, after coupling them based on their interdependence, this paper will examine if the alliance could easily: define a proactive and anticipatory strategy for the Black Sea; define and end-state supported by political purpose; find a balance between objectives, methods and resources; define a strategy based on hierarchy, comprehensiveness and knowledge of the environment. An exception in building this framework is including the last premise identified by

Yarger, which is more of a description of the effects of strategizing, so it remains just something to keep in mind as to why NATO would benefit from involving in this endeavour.

Can NATO easily define a proactive approach to the Black Sea?

The Black Sea region is already an area of strategic importance, considering that even if the premises of a NATO-Russia conflict have not been established after Russia's full-scale invasion of Ukraine in 2022 or after illegally occupying Crimea, because Ukraine is not a NATO member, the threat continues to persist over this part of the eastern flank. It is indicated by numerous provocative actions. Just to name some, Russia's hybrid war against the NATO coastal states Romania and Bulgaria, facing new risks of escalations with Russia's drone attacks near their borders and new warning areas in the Black Sea, and the proximal combination of invasions, territory occupations, and hybrid threats used against the Euro-Atlantic aspirant states from this region: Ukraine, Moldova, and Georgia, since the fall of the USSR.

In this complex environment, NATO lacks a Black Sea strategy to show its views of "the smallest set of choices to optimally guide other choices" (Van den Steen, 2013, p. 1). Since 2022, NATO has had a lot of choices to make concerning this region, thus, most likely, NATO members are already capable of a proactive and anticipatory approach to the Black Sea. This is because, as they have engaged with multiple crises in this area and are engaging in deterrence efforts, they can recognise patterns and anticipate potential future ones. With this ability, the Alliance can define how it will take initiative to improve the situation or to create a new one, which is a definition of proactive behaviour (Bateman and Crant, 1993). This is a valid assumption also because the Black Sea is historically a place for increased competition between the global powers and it has been, for a long time, the barrier between the East and the West (Altin, 2024).

The region is still the barrier between NATO, a presence in this area since 1952, and Russia; the meeting point of allies' efforts to deter Russia and Russia's efforts to keep the ex-USSR states in this region as a buffer zone. Therefore, since 2014, after Russia's illegal annexation of Crimea, both have raised their military capacities in the area. On one

side, Russia strengthened its land-based early warning and armament systems, as well as equipped its Black Sea Fleet with long-range land and sea missiles (Altin, 2024). On the other side, NATO started air policing over the Black Sea and NATO states land territory, forming for the first time NATO battle groups in Romania, Bulgaria, and Hungary. NATO is enhancing its presence by placing two multinational battle groups in Romania and Bulgaria and increasing air patrolling of the sea for securing oceanic routes, infrastructure denial for securing the undersea facilities in the future, by the help its members provided for Ukraine, and by establishing the NATO–Ukraine Council and coordination with regional and international partners.

NATO having this significant presence in the Black Sea Region is a clear sign of the allies being able to anticipate a need for future defence, even if its position and credibility might depend on its future actions regarding expansion and resolving the ongoing and frozen conflicts in the region. In these regards, a strategy can show how members will use their means and resources to exercise control over these challenges, proving that the alliance doesn't seek escalation in the area, but firmly engages in building the defensive capacity of the riparian states.

For example, although a possible efficient approach to build up defensive capabilities would be to plan for NATO's possible expansion and a possible continuous naval presence in the Black Sea, backed by naval infrastructure, this will most likely be seen by Russia as a threat. A strategy could show the allies vision on how the members will increase the defence capacity, without straying from a defensive nature and increasing the chances of the region turning into a perpetual zone of conflicts.

Nonetheless, agreeing on "how" to achieve defence objectives in this region seems still very difficult, as there are still questions about even the riparian allies coming to common grounds or uniting to support an initiative.

Despite intra-alliance challenges that will be reviewed in the next chapter, NATO has taken consistent steps to enhance its presence and to increase regional cooperation, which can only demonstrate that the members possess the knowledge, instruments and capacity to clarify "how" the alliance will manage defending the area, not just to make it

able to react. NATO has a decades-long track record of training on recognising early warning signs in this area, of building presence, and maintaining operational continuity, even amid diverging member interests. Thus, theoretically, the first premise of a theory of strategy – "strategy is proactive and anticipatory" – could be easily established by the alliance in such an endeavour, bringing us one step closer to a Black Sea strategy.

Can NATO easily define an end-state supported by common political purpose in the Black Sea?

Defining what is to be accomplished by the allies in a Black Sea Strategy should not prove to be an impossible challenge, as they are already defined as a defensive alliance, they have already expressed the strategic importance of the area and some members are even more advanced in defining their purposes in national policy documents. Thus, besides common declarations and strategic documents, some allies have engaged in defining their political purpose in the area, the expression of the desired end-state sought by their government at some point in the last decade. Similar to how the difference in terms of power and ambition to project political purposes have determined different desired end-states in documents like national security strategies of the riparian states, the same phenomenon probably will probably occur when defining the common desired end-state. So this task might be more complicated.

Driven by the escalation in Ukraine, after the Madrid NATO Summit, on 29 June 2022, NATO released a new Strategic Concept that sets the Black Sea region as an „area of strategic importance for the Alliance", also acknowledging "Moscow's military build-up" (NATO, 2022, pp. 4-11) in the region, but this was not followed by properly developing a strategy for this critical flank of the alliance. Allies recognised again the strategic importance of the Black Sea region at their summit in Vilnius in July (NATO, 2023), for the first time in a summit communique, and the most relevant initiative in the Black Sea since then was scaling up the military presence in this eastern flank to multinational battalions in Romania and Bulgaria (DSCFC of NATO PA, 2023).

At an individual state level, The US Congress enacted in March 2023 a bill that called upon the security agencies to agree on a Black Sea

security strategy, the "Black Sea Security Act of 2023" (Congress.gov., 2023). The Act recognises the critical role of littoral states in contributing to the collective security of NATO and Russian expansionism as a threat to the national security of the United States and NATO. It also calls for NATO to develop a long-term security strategy for the eastern flank, a rotational maritime presence in the Black Sea, and Turkey to avoid future actions that could escalate tensions in the region and states the commitment to support and bolster economic ties with the Black Sea states, encouraging the advance of the Three Seas Initiatives. For the US, it seemed important, at that point, to increase cooperation, to prioritise intelligence gathering, to evaluate the challenges and opportunities for new forms of military presence in the Black Sea, or to engage in combating the Russian disinformation in the region. Even if the US desired end-state for the Black Sea might change, the document still offers a scenario to build on through negotiations.

The riparian states of the Black Sea themselves have a history of conflicts throughout history, starting with the involvement in the Russo-Ottoman wars on opposite sides, which will probably influence their suggestions on the desired end-state, as we can already see from differences in their national security strategies. If we consider their strategies an expression of their political purpose in engaging in defending the Black Sea, we can see some different approaches.

Considerations on the political purpose of Romania for a Black Sea

Being closer to the problem, Romania's National Defence Strategy asserts that, in the face of Russia's actions directed at ensuring control of the Black Sea, the country is dedicated to being a pillar of regional stability (RNDS, 2019-2024, p. 9) and engages in raising awareness among allies about the Black Sea region's importance in the security architecture, promoting its potential as an energy and transport corridor, while projecting its ambitions as a regional actor in the energy supplies, due to the energy resources possessed in the Black Sea. According to its national defence strategy (2019-2024), Romania puts its NATO and EU integration as its greatest achievement in 30 years and clearly states the

national commitment to guarding the eastern frontiers and the Black Sea but also underlines the strategic partnership with the US. Also, the country acknowledges the Russian aggression, the hybrid war it conducts – considered to be a rising risk compared to an armed conflict between states – and its efforts to militarise the Black Sea and so commits to continue its efforts to build deterrence and defence capabilities. For solving the defence and security problem in the region, Romania envisions a strategy that consists of increased allied defence and deterrence on the eastern flank, equally from the north to the south; EU unity in action; and the US committed to the security of the Black Sea. From a national point of view, Romania seeks to reaffirm the importance of the Black Sea for regional security and states that the country must engage in communicating this for maintaining and increasing the attention of 3 actors upon the Black Sea – NATO, the EU, and the US (RNDS, 2019). The strategy also considers that Romania should promote Euro-Atlantic integration in the Black Sea, especially in Moldova, Ukraine, and Georgia.

Considerations on the political purpose of Bulgaria for a Black Sea Strategy

According to Bulgaria's National Defence Strategy (2023-2033) and National Security Strategy (2018), the country is much more focused on national interests that can be achieved through meeting NATO and the EU's objectives regarding military and civilian capabilities. The war in Ukraine influenced the defence strategy, and the events in the Black Sea encouraged a vision for solving the defence needs by prioritising the fulfilment of allied commitments. Bulgaria defined Russia as the main threat, similarly to Romania, not just in military terms but also through informational-psychological, political, and economic impact, which means hybrid threats, also stating that the potential for conflict in the Black Sea will be high in the long term, with territorial disputes continuing to put pressure on the area. The Bulgarian strategy defines and priorities the country's potential for deterrence and defence, similarly to Romania, and possible missions under Article 5, while also committing to at least 2% of GDP spending on defence from 2024 (China-CEE Institute, 2023).

Considerations on the political purpose of Turkey for a Black Sea strategy

On the other hand, Turkey's National Security Policy Document is not public, but after the 2018 elections and the country becoming a presidential republic, similar concerns about the war in Ukraine are now linked to the country's national security in the view of the government (Li, 2024). What strongly differentiates Turkey's security policies from Romania and Bulgaria is the influence of two contradictory identities within the country: a westernised and secularised west coast and a conservative, more attached to Islamic traditions and economically underdeveloped east.

Under Recep Tayyip Erdoğan, Turkey seems more concerned with balancing between Europe and the Middle East and Central Asia, emphasising maritime interests and modernising the naval forces (Li, 2024), which could benefit balancing Russia in the Black Sea, but it depends on how successful a strategy based on duplicity can be and how it manages to resolve its most important internal problems related to ethnic separatism. The duplicity was already proven in NATO matters when Turkey used the context provided by the war in Ukraine by leveraging its veto rights to demand candidate countries Finland and Sweden allow weapons exports and end support for Kurdish forces and the PKK.

After 2006, Turkey's relations with both EU and NATO have become increasingly strained due to diverging political priorities, regional disputes, and security concerns. These developments have raised questions about Turkey's alignment with Western institutions and its long-term strategic orientation.

Much different than Romania and Bulgaria, Turkey is prioritising increasing its independent defence industries and military capabilities, not relying on western support, as the divergences with western countries were growing after multiple arms embargoes and the failed *coup d'état* in July 2016 (Li, 2024, p. 72) and, more recently, undermining sanctions against Russia, being a supplier of dual-use items to Russia, and purchasing Russian S-400 air defence systems (Smith, 2020), which led to its exclusion from the F-35 fighter program and sparked concerns over NATO interoperability and security. Further frictions arose from Turkey's

delay in ratifying Sweden's NATO accession, citing concerns over Kurdish militant support, as well as its pursuit of an increasingly autonomous foreign policy that includes close ties with Russia and unilateral military interventions in Syria and Libya.

EU accession negotiations have been frozen since 2018, largely due to democratic backsliding, the erosion of judicial independence, and human rights violations. Also, Turkey's explicit refusal to recognise Cyprus is a core issue that continues to strain its relations with the EU, leading to the suspension of negotiation chapters regarding the internal market since 2006.

While NATO has recognised the strategic significance of the Black Sea, defining a cohesive and commonly supported end-state will be a challenge, shaped by diverse national interests, historical legacies, and geopolitical calculations. We can catch a glimpse of these differences looking at the riparian members. Therefore, the formulation of a common end-state for the Black Sea strategy is not unattainable, but requires major negotiation to achieve a deeper common political purpose, besides the pledged commitment to collective security principles. But maybe the most important part, due to the current security environment, is adopting a strategy for the security of this region and communicating NATO's focused views on what is still to be accomplished in the region in order to defend its members to the world. This could help combat the psychological warfare and also improve the perception of the alliance's usefulness in the area, providing the ways to compete with Russia "for the aspirations of citizens in the Black Sea region" (Gaber, 2024), as experts observed in 2024's Romanian Parliamentary Black Sea Forum and Black Sea Security Conference in Bucharest, mainly because of increasingly observed hybrid threats and communications deficiencies of the allies regarding the area.

Can NATO easily find balance among objectives, methods, and resources in the Black Sea?

This will require that for every type of objective, NATO must define concepts and use resources available for it. So, for example, if an

objective has a stronger impact on just one ally, the methods and resources considered should be proportional to the national level.

Objectives for the Black Sea. After the Vilnius Summit, the allies have already defined some approaches to the Black Sea (NATO, 2023), which can be considered for a possible integration in a future focused strategy:

- supporting Ukraine in the long term, keeping in mind the "as long as it takes" (NATO, 2023) commitment, first regarding NATO membership and second with non-lethal assistance.
- supporting Moldova with its European integration and Georgia to advance its Euro-Atlantic path, as agreed at the 2008 Bucharest Summit.
- developing their own national Black Sea strategies by which they can underline their interests and how they can contribute to an allied strategy. Together, these states can first promote bringing up to date the Strategic Action Plan for the Rehabilitation and Protection of the Black Sea (1996).
- possible cooperation in improving military mobility by improving the infrastructure (railways, highways, and port facilities) to ensure suitability in case of the need to use it for military purposes.
- increased naval presence, air missions, rotational presence of ground forces, increased exercises and trainings, building defence capacity for partners, enhancing strategic communication, and infrastructure protection tasks and missions (Horrell, 2016), fields in which we can see improvements after 2022 or, at least, raised concerns about ways to improve.

A strategy can show, in more detail, the objectives NATO considers in order to prevent or to respond to another crisis in the Black Sea region. Having clear strategic objectives in the area, collectively agreed upon in times of non-crises, the allies would be better equipped in decision-making and this could bolster cooperation, clarifying the level of threat and the level of retaliation it should face.

Adapting the methods. Methods will constitute the ways to achieve the objective of the alliance and, a particular aspect to consider in a future strategy will be to plan according to international law.

International law is of crucial importance in the Black Sea, starting with the Montreux Convention. In the interest of putting forward a successful strategy, the allies must previously be involved in analysing how to use the advantages and disadvantages of international law, for meeting their purposes in the area and for adapting the capabilities they possess and measures them can engage in.

Although a lot has changed in the Black Sea security environment since the great power's strategic competition, the Montreux Convention, signed by Australia, Bulgaria, France, Greece, Japan, Romania, former Yugoslavia, Turkey, the United Kingdom, and the Soviet Union in 1936, still governs the transit of vessels through the Turkish Straits, which links the Mediterranean to the Black Sea and helps maintain a rules-based international order in this region.

Since Turkey joined NATO in 1952, this strait has been under the control of a NATO state. This is, at least theoretically, an advantage, as a NATO ally has the power to impose various degrees of restrictions on all warships passing through and has access to information about them, an advantage that could be used to deter Russia's efforts to gain dominance in the Black Sea. Turkey proved the strategic importance of this Convention on the February 27, 2022 by invoking article 19 and declaring the situation in Ukraine a war, blocking Russia's possibilities to reinforce the Black Sea fleet with ships from other fleets (DSCFC of NATO PA, 2023). Also, Turkey closed the Black Sea to all non-Black Sea riparian state warships in line with the Montreux Convention.

Developing a NATO naval flotilla operated by NATO littoral states (Chiriac and Theresheva, 2016) would ensure compliance with the Convention but requires an agreement between them, large participation of Turkey, and analysing and overcoming budget and political constraints. Also, Romania and Bulgaria, as NATO allies, can approach the need for an increased presence in the Black Sea by exploring the use of the Danube River and the Danube-Black Sea Canal, as Germany is a Danubian state with a navy that can be invited by Romania into its sections of the Danube River, according to the 1948 Convention Regarding the Regime of Navigation on the Danube (Sloan, 2020). Also, for such an opinion to be available, at full potential, Romania and NATO must work together on modernising the canal for military use, as for now it is relatively small

(Coffey, 2020). But all these efforts would require not just initiative and cooperation, but also financial capacity and political will. There could be negotiations for securing EU funding or support through NATO's common funding mechanisms, based on clear and shared commitment to making inland waterway access a credible component of regional deterrence and mobility, but there is no public indication of a strong political will from any NATO member, the common focus being on mobility via land and air.

Considerations on the resources. Resource allocation differs significantly, as seen among NATO members in the Black Sea region (Becker, 2019 and 2021). Any strategy for sharing the collective defence burden for this region must therefore account not only for defence capabilities but also for broader geopolitical and economic considerations aimed at preventing future large-scale conflict. One such approach involves fostering economic integration with all actors in the region (Amilakhvari and Baghaturia, 2023). While politically sensitive – especially when sanctions are required – economic interdependence could be a long-term stabilising factor, potentially reducing the pressure on NATO to maintain high levels of defence spending indefinitely.

Achieving this, however, goes beyond NATO's military mandate and requires cooperation with the European Union, which has the institutional tools to promote regulatory alignment, democratic governance, and economic development. The EU's involvement is essential for addressing structural challenges and advancing regional stability in non-military domains. At present, even NATO members in the region – Romania, Bulgaria, and Turkey – do not uniformly benefit from the same level of integration into EU political and legal frameworks, which limits their ability to promote a cohesive model of governance and stability across the wider Black Sea. Bridging this gap requires a coordinated NATO-EU effort to align security goals with political and economic transformation.

But when it comes to the allocation of military forces, the task seems easier, as France and Italy are serving as the framework nations for the multinational battle group stationed in Romania and Bulgaria, with Belgium, Luxembourg, the Netherlands, the Republic of North Macedonia, Poland, Portugal, the United States, Albania, Greece, Montenegro,

Macedonia, and Turkey as contributors. The United States also relocated in 2022 an additional 1.000 soldiers from bases in Germany to Romania, bringing the total number of stationed US forces in the country to approximately 1.900 (Romanyshyn, 2023). Later in the summer, the United States rotated in an additional 4.000 soldiers from Mihail Kogălniceanu Air Base, near Romania's major Black Sea port, Constanta, doubling the amount of NATO forces stationed in the region (NATO, 2022).

NATO member states have also increased their air defence systems within the Black Sea region, including increased fighter jets, ground-based air defence systems, and surveillance flights (NATO, 2022) and, prior to Russia's full-scale invasion of Ukraine, the allies sailed warships in the Black Sea and have tried to increase intelligence collection and military mobility to be prepared for any escalations. Also, Romania and Bulgaria are investing in expanding their maritime capabilities and defence capabilities by announced acquisitions of submarines and patrol ships.

NATO's ability to balance objectives, methods, and resources in the Black Sea will depend on complex legal, political, and regional constraints, but there is a solid foundation to build on, as some objectives have been clearly outlined, there are creative methods to achieve even ambitious defence objectives and the alliance has improved the resource, at least in terms of military presence and capabilities, that it can use in the region.

Can NATO easily define a strategy based on hierarchy, comprehensiveness and knowledge on the environment for the Black Sea?

These attributes will also define the success of a future strategy in an interdependent way. A hierarchy will not translate into coordinated action without comprehensive planning and knowledge about the Black Sea. Comprehensive thinking will assure that the strategy is not focused on just one aspect of collective-defence (like military capabilities) and deep knowledge will help the alliance strategize on assumptions deeply based on reality. NATO already approaches the Black Sea based on these three, to an extent.

Replacing hierarchy with consensus-based. If we consider that a strategy has to be hierarchical, the process will be challenging because

32 sovereign countries will have to develop a strategy in a consensus-based, politically multi-layered and military process. So, instead of a purview of a leader as a "weltanschauung" (world view) that represents both national consensus and comprehensive direction" (Bartholomees, 2006), NATO would have to present the view of the 32 states. At most, the requirement of hierarchical nature will be applicable in the part of the process involving the military structure and when applying the strategy, especially during joint operations.

Therefore, for NATO to have a strategy on the security of the Black Sea, as the consensus would be mandatory, a common stance of the riparian members on regional security matters might speed up diplomatic negotiations that precede such a realisation. As the Black Sea Economic Cooperation (BSEC) and other multilateral platforms in the region – like the GUAM (Georgia, Ukraine, Azerbaijan and Moldova) Organisation for Democracy and Economic Development and the South-Eastern Europe Brigade (DSCFC of NATO PA, 2023) – have failed to make a clear difference on large impact security issues, focusing on economic cooperation, and Russia's revisionism is increasing since 2000, there is a need for a strong form of continuous dialogue on security that can be achieved if NATO states commit to such kind of strategic approach, instead of limiting their cooperation to punctual security operations, like the Mine Countermeasures Black Sea (MCM BLACK SEA) Task Group.

Turkey is a plausible candidate to drive cooperation among the allied littoral states, given its significant military and naval capacity that could support a leadership role, but the aspects described in relation to its political purpose in the Black Sea might prevent it to assume this role.

Comprehensiveness and deep knowledge on the Black Sea security environment

Both the comprehensiveness and the knowledge that will be the foundation of a strategy are related to NATO operating in an environment – in this case, the Black Sea region, which it can impact, but also will impact its efforts continuously, meaning that NATO must be cognisant of its own way of functioning, at all levels, and with all the aspects that it interacts with it. This includes national military strategies, national security strategies, national interest and the external environment, which must be put through analysis to find the factors that will help and

the ones that will affect the end-state (Bartholomees, 2006). Throughout these papers, the national aspects that might impact the form of the strategy were brought to light, after being identified in public sources, meaning that they are well known and NATO can easily take them into account. This is also valid for the knowledge of the external (to NATO) environment, about which some aspects might be a little more relevant in a future strategy.

First, even if Russia, the obvious threat source for NATO in the Black Sea, does not itself have a strategic document revealing a strategy for the Black Sea Region, NATO is not in a position to follow its example. Opposed to Russia, it can't rely on traditional approaches, as its position of proactive key actor in the area before 2022 is questionable and, more, its presence in this area consists of countries with more or less different approaches to security and defence. Russia has an approach to foreign policy that is deep-rooted in its long history of being a superpower of the region, but Romania, Bulgaria, and Turkey don't share a common perception of the Russian revisionist threat. To add to that, historically, before 2014's illegal annexation of Crimea, key NATO members governments showed rather less interested in Black Sea security (being more focused on the Baltic Sea security, East Asia and the Pacific, the Middle East, or particular threats, such as migration), although that changed very recently, to be more specific, since 2022, which can be understandable considering that for the western allies the danger might be perceived less imminent, but it has left the impression of a late strategic shift.

Some of the objectives noticed by experts regarding Russia's strategy in the Black Sea (Chindea, 2019) are: separating Turkey and Bulgaria from NATO and EU through economic and energy weaponization, spreading false narratives that would diminish the western support for Ukraine inclusion in NATO, including the threat of nuclear weapons, or deepening control over Crimea to maintain a gateway to control the Black Sea and threat all the littoral states by securing a base for long-range cruise missiles and coastal defence capabilities. Russia does all these while also maintaining or encouraging conflicts in Georgia, Moldova, Ukraine, and Azerbaijan and interfering in other countries foreign policies, including Romania, Bulgaria, and Turkey.

These are all part of the hybrid war conducted by Russia on the Black Sea countries. According to the chief of the general staff of the Russian Armed Forces and first deputy defence minister, Valery V. Gerasimov, in modern wars, to reach the political goals, it is not enough to use military forces and traditional tactics, but a combination of military means and non-military measures is needed, which shows the Russian approach to hybrid warfare even without even using the term (Mikac, 2022). It has the particularity that its tactics can go unnoticed by the population but still affect all aspects of society and life, in particular politics, diplomacy, economy, and cyber or information. For example, disinformation campaigns are often conducted by inauthentic accounts or local proxies, gradually shaping public opinion and deepening polarisation without clearly revealing their foreign origin. Hybrid war exploits economic vulnerabilities of the area, creates ambiguity by masking the true intentions of the attacker, and is conducted through state and non-state actors against the other riparian states, including through overt or covert actions that affect physical or psychological targets, inflicting fear in the population.

All NATO states are a target of Russia's hybrid war because of its usefulness in degrading the willingness to confront the aggressions conducted in the region and in furthering foreign policies from the Euro-Atlantic path. This means a NATO security strategy for the Black Sea cannot ignore dealing with the hybrid threats and the hybrid war, a term familiar to the alliance, as it shows concern about growing hybrid threats, as they soften the lines between war and peace. This would not be a duplication of EU efforts, but rather complementing them by leveraging NATO's unique strengths: strategic intelligence-sharing, civil-military coordination, cyber defence capabilities, and infrastructure resilience planning.

For example, in Romania, the most present examples of hybrid threats of Russian source could be disinformation and related types of psychological operations, like deception through the Grand Pro-Putin Narratives combined with breaches of the airspace and exploitation of the fear of war, while in Bulgaria is the distortion of history to portray Russia as a protector and liberator, the belongingness to the "Slavic family," or exploiting the tangible dependence on Russian gas (Hadzhiev,

2020). Also, there are similar tactics like the division of the population, for example, in Russophiles and Russophobes in extreme cases, nurturing the feeling of nostalgia towards the times of these countries being USSR's satellites, and different levels of political instability, but still both experiencing governance shortcomings (Hadzhiev, 2020). The Grand Pro-Putin narratives in Romania focus more on influencing the perception of Romanians toward the east, as the feeling of friendship toward Russia is harder to directly appeal to, by blaming the war on Ukraine on NATO's enlargement, nurturing revisionism, and the lack of a voice and benefits in the EU (Expert Forum, 2024).

It is psychologically reassuring that in 2016 NATO publicly stated that hybrid actions against one or more Allies could lead to a decision to invoke Article 5 of the North Atlantic Treaty, but the primary responsibility to engage with the threats or attacks is within the targeted country (NATO, 2024). Hereupon, there is no strategic guidance for the threshold above which a call for Article 5 is justified and the equitable response, which leaves the Black Sea allies, just like all allies, in an uncertain position, but closer to a specific area of interest for Russia. Fighting back with the same weapons against the Russian hybrid war is a sensitive topic that must be well analysed so the strategic directions don't lead to escalations. Also, strengthening the intelligence-gathering capabilities and cooperation between BS NATO members and candidates can help have an efficient early warning system, but also avoid limited interoperability or operational gaps. For example, the interoperability within NATO's artificial intelligence (AI) strategy, particularly concerning Turkey, has been questioned (Anadolu Agency, 2023) after the rapid development of AI-based military drones in Turkey. On this basis, engaging with Turkey must be done on a deep basis of understanding its need for acknowledged strategic autonomy in this area.

In conclusion, while NATO may not be able to construct a hierarchical strategy for the Black Sea, but more of a consensus-based one, it looks like it can easily build a coherent and actionable framework rooted in a deep understanding of all the layers of this security environment.

Conclusions

Having a critical frontline for deterring Russian aggression in the Black Sea, a geopolitical space of high levels of uncertainty and propensity to conflicts, the allies are responsible to themselves to come up with a clear security strategy for the Black Sea. Likewise, the riparian allied states – Romania, Bulgaria, and Turkey – are well positioned to identify and propose concrete measures to address the challenges posed by Russian expansionism, which is manifested through the illegal annexation of Crimea, the ongoing war in Ukraine, and the continued occupation of Georgian and Moldovan territories.

The aim of this paper was to assess NATO's readiness to release a Black Sea strategy. The theoretical foundation of this analysis was Yarger's paper on a theory of strategy (Bartholomees, 2006), which outlines seven premises to build a strategy. These premises were synthesised into four questions about NATO's ability to easily meet the potential requirements, as following:

- Can NATO easily define a proactive approach to the Black Sea?
- Can NATO easily define an end-state supported by common political purpose in the Black Sea?
- Can NATO easily find balance among objectives, methods, and resources in the Black Sea?
- Can NATO easily define a strategy based on hierarchy, comprehensiveness and knowledge on the environment for the Black Sea?

The research has examined the benefits, challenges, current progress, and key focus areas to consider, by analysing academic literature and official documents. Special attention was paid to analyse the views and contributions of Romanian, Bulgarian, and Turkish, as the riparian states most impacted by the evolutions in the region. Their national positions were compared and contrasted and showed different understandings of the environment and capabilities that might need to be addressed.

To summarise, the research on these questions has shown that NATO already possesses several foundational elements necessary to formulate a Black Sea strategy, as defined by Yarger's theoretical framework. On all the matters addressed, challenges are reconciling

national interests, constructing a strategy through consensus, and the topic that appears to be the most significant hurdle is political alignment. Nonetheless, groundwork laid in recent years suggests that, with deliberate coordination and sustained diplomatic effort, NATO could successfully translate its current capabilities and experience into a focused regional strategy. The alliance has the reasons, the means and the understanding required to collectively define an approach to the Black Sea, a common view on a viable alternative to the risks posed by unchecked Russian revisionism.

This suggests that NATO is prepared in many ways to release a Black Sea strategy – in terms of identifying and presenting an approach based on proactive behaviour, purpose, balance, and a deep understanding of the dynamics in the region. However, the alliance seems to lack in terms of political will. Despite being deeply engaged in the region after 2014, the absence of official discourse on such a strategy over the past eleven years show that progress will continue to be slow if political unity remains elusive. This indicated the need to unify the allied views and actions regarding this area.

Ultimately, there are a lot of research questions left, for example, "Is Türkiye a reliable partner for building a strategy with it as a key regional player?" or "What would strongly encourage the rise of such a common political will?" but this research shows, at least, the potential progress in having a NATO strategy for the Black Sea.

References:

1. Amilakhvari, L., and Baghaturia, O. (2024). "Georgia's Place on the Brzeziński 'Grand Chessboard' Amidst Growing Geopolitical Turbulences," in National Defence Academy of Georgia, *International collection of the papers of the scientific-practical conference: South Caucasus and Black Sea Security Conference* (pp. 167-177). https://eta.edu.ge/uploads/2024%20Konferenciebi/South%20Caucasus%20and%20Black%20Sea%20Security%20Conference.pdf#page=213

2. Anadolu Agency. (2023, January 29). "Turkish firm chosen to develop 'critical' NATO intelligence software." *Anews*. https://www.anews.com.tr/world/2023/01/29/turkish-firm-chosen-to-develop-critical-nato-intelligence-software

3. *Arhitectura dezinformării româneşti: Relația cu Kremlinul [The architecture of Romanian disinformation: The relationship with the Kremlin].* (2024). Expert Forum. https://expertforum.ro/en/files/2024/09/Arhitectura-dezinformarii-romanesti-Relatia-cu-Kremlinul.docx-1.pdf-1.pdf-en.pdf.

4. Atlantic Council. (2020). *A NATO strategy for security in the Black Sea region*. Centre for Security Studies, ETH Zurich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/Atlantic%20Council-A%20NATO%20Strategy%20for%20Security%20in%20the%20Black%20Sea%20Region.pdf.

5. Altin H. (2024). "Revisiting the importance of the organization of the Black Sea economic cooperation (BSEC) in a changing regional and international geopolitical landscape." *Journal of Political Administrative and Local Studies*, 7(1), 14-32. https://doi.org/10.17550/jpal/1480779.

6. Bartholomees, J. B. (Ed.). (2006). *U.S. Army War College guide to national security policy and strategy* (2nd Ed.). U.S. Army War College Press. https://press.armywarcollege.edu/monographs/78.

7. Bateman, T. S., and Crant, J. M. (1993). "The proactive component of organizational behaviour: a measure and correlates." *Journal of Organizational Behaviour*, 14(2), 103–118. https://doi.org/10.1002/job.4030140202.

8. Becker, J. (2019). "Burden-Sharing, Geopolitics, and Strategy in NATO's Black Sea Littoral States." *SSRN Electronic Journal*. https://www.researchgate.net/publication/344963074_Burden-Sharing_Geopolitics_and_Strategy_in_NATO's_Black_Sea_Littoral_States.

9. Becker, J. (2021). "Defence spending, burden-sharing and strategy in NATO's Black Sea littoral states: domestic, regional, and international systemic factors." *Southeast European and Black Sea Studies,* 21(3), 393–413. https://doi.org/10.1080/14683857.2021.1906942.

10. China-CEE Institute. (2023). *Bulgaria: An important partner in China's Belt and Road Initiative.* China-CEE Institute. https://china-cee.eu/wp-content/uploads/2024/05/2023p10_Bulgaria.pdf.

11. Chiriac, M., and Theresheva, M. (2016). "Black Sea flotilla fiasco worsens region's tensions." *Balkan Insight*. https://balkaninsight.com/2016/06/28/black-sea-flotilla-fiasco-worsens-region-s-tensions-06-27-2016/.

12. Coffey, L. (2020). "To Boost NATO's Presence in the Black Sea, Get Creative." *Defence One*. https://www.defenseone.com/ideas/2020/05/increasing-natos-presence-black-sea-time-get-creative/165760/.

13. Congress.gov. (2023). *S. 804 - A bill to impose sanctions on the Russian Federation in response to its aggressive actions in the Black Sea region*. https://www.congress.gov/bill/118th-congress/senate-bill/804/text.

14. Gaber, Y. (2023). *New security reality: Strategic approaches to the wider Black Sea region.* George C. Marshall European Centre for Security Studies. https://www.marshallcenter.org/en/publications/clock-tower-series/new-security-reality-strategic-approaches-wider-black-sea-region/new-security-reality-strategic-approaches-wider.

15. Hadzhiev, B. (2020). "Enablers of hybrid warfare: The Bulgarian case." *Journal of International Studies*, 13(1). https://doi.org/10.14254/2071-8330.2020/13-1/2

16. Hodges, B., Horrell, S., and Kuz, I. (2022, September 22). *Russia's militarization of the Black Sea: Implications for the United States and NATO.* Centre for European Policy Analysis. https://cepa.org/comprehensive-reports/russias-militarization-of-the-black-sea-implications-for-the-united-states-and-nato/.

17. Horrell, S. (2021). *A NATO strategy for security in the Black Sea region.* Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-nato-strategy-for-security-in-the-black-sea-region/

18. Li, Y. (2024). *Turkish National Security Strategy: Evolution, Characteristics, and Practices.* China Institutes of Contemporary International Relations.http://www.cicir.ac.cn/UpFiles/file/20240719/638569802487423 6145056414.pdf.

19. Mikac, R. (2022). "Determination and development of definitions and concepts of hybrid threats and hybrid wars: Comparison of solutions at the level of the European Union, NATO and Croatia." *Politics in Central Europe,* 18(3), 355-374. https://doi.org/10.2478/pce-2022-0016.

20. NATO Parliamentary Assembly. (2023). *Black Sea security and regional stability: Lancaster report* (DSCFC 23 E rev. 1). https://www.nato-pa.int/download-file?filename=/sites/default/files/2023-10/020%20DSCFC%2023%20E%20rev.1%20fin%20-%20BLACK%20SEA%20-%20LANCASTER%20REPORT.pdf.

21. *NATO 2022 strategic concept*. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

22. *NATO's approach to the Black Sea region*. NATO. https://www.nato.int/cps/en/natohq/topics_156338.htm

23. Porter, M.E. (1996). "What Is Strategy?" *Harvard Business Review*. https://cdn.paynevesht.ir/assets/2_af58ff4da6.pdf.

24. Romanian Presidential Administration. (2020). *Strategia Națională de Apărare a Țării 2020-2024 [National defence strategy of the country 2020-2024].* Romanian Presidential Administration. https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf.

25. Romanyshyn, I. (2023). Ukraine, *NATO and the Black Sea*. In NATO Defence College, *NDC Policy Brief*. https://www.cassis.uni-bonn.de/de/publikationen/ukraine-nato-and-the-black-sea/ukraine-nato-and-the-black-sea/@@download/file.

26. Sloan, S. (2020). Increasing NATO's presence in the Black Sea: It's time to get creative. *Defence One*. https://www.defenseone.com/ideas/2020/05/increasing-natos-presence-black-sea-time-get-creative/165760/.

27. Smith, S. (2020). U.S. sanctions Turkey over Russian S-400 missile defence system. *CNBC. https://www.cnbc.com/2020/12/14/us-sanctions-turkey-over-russian-s400.html*

28. Van den Steen, E. (2017). "Strategy and the Strategist: How It Matters Who Develops the Strategy." *Management Science*, 64(10):4533-4551. https://doi.org/10.1287/mnsc.2017.2857.

INTELLIGENCE, SECURITY AND INTERDISCIPLINARITY

THE ROLE OF ARTIFICIAL INTELLIGENCE IN PREVENTING DIGITAL TRAFFICKING OF CULTURAL ARTIFACTS

Alexandra NICOLESCU*

Abstract:

The adaptation of cultural crimes to the digital environment has enabled terrorist groups and criminal networks to exploit online platforms, social media and encrypted applications for the illicit trafficking with cultural artefacts. This article explores how artificial intelligence may contribute to preventing and disrupting digital trafficking of cultural objects. The research explores how emerging technologies, such as image recognition, metadata analysis and algorithmic mapping tools, can contribute to the identification and monitoring of these crimes.

The aim of this research is to assess the capacity of artificial intelligence to detect suspicious transactions and support investigations, as well as to analyse the legal and technological barriers that limit its application. The study adopts an interdisciplinary approach that integrates legal, technological and cultural perspectives, and proposes innovative solutions to enhance the effectiveness of these technologies.

The findings show that artificial intelligence can play an important role in protecting cultural heritage, though its impact is limited by incomplete databases, the fragmentation of information, and confidentiality matters. At the same time, collaboration between experts and algorithms, along with the implementation of federated learning, can enhance both the efficiency and the credibility of AI-based solutions.

Keywords: *cultural terrorism; illicit traffic; artificial intelligence; international legislation; funding sources; digital commerce.*

Introduction

At present, the illicit trafficking and trade of cultural artefacts has become a serious threat to international security and the preservation of the world's cultural heritage. These illicit activities have evolved from being primarily associated with private collectors and art markets to

* PhD student in Security Studies and International Relations, Babes-Bolyai University, Cluj-Napoca, email address: alexandranicolescu9718@gmail.com

serving as a significant source of funding for terrorist groups (Kersel and Gerstenblith, n.d.).

The fight against the illicit trafficking and trade of cultural artefacts is now a priority for the international community, leading to legal and political initiatives and to the exploration of technological solutions. In this context, artificial intelligence is recognized as a strategic tool in international efforts to prevent and combat the illicit trade of cultural property.

This research seeks to analyse the role of artificial intelligence (AI) in preventing and combating the digital trafficking of cultural artefacts.

The objectives of this study aim to:

1. Examine how artificial intelligence can be applied to detect suspicious online activities and track cultural artefacts sold online.
2. Review the international legal framework on digital trafficking of cultural property and assess the contribution of AI to prevention efforts.
3. Identify the main challenges and limitations in implementing artificial intelligence tools in this field and to suggest innovative ways to improve the use of these technologies.

This study adopts an exploratory qualitative approach, based on the analysis of secondary sources related to the fields of cultural heritage protection, transnational crime and emerging technologies. The research uses a documentary method, which includes identifying, selecting and critical interpretation of information from scholarly literature, international legislation, institutional reports and investigative journalism.

The research draws on a variety of sources, including scholarly studies from the international academic literature, articles from the international press and normative acts issued by global organizations.

The issue of digital trafficking of cultural objects has been highlighted both in press articles and in international academic research, which has documented the use of social networks, encrypted applications and online marketplaces for the promotion and sale of illicit goods. However, academic studies have only recently started to address the technological dimension of these cultural crimes and the use of

artificial intelligence to prevent and combat the digital trafficking of cultural artefacts remains insufficiently explored.

In this context, the study aims to offer a clearer picture of AI's role in countering digital trafficking of cultural heritage, by examining both its potential benefits and the obstacles that may hinder its effective use.

This study makes a contribution by connecting legal and technological perspectives. It highlights the gaps in legislation regarding the digital trafficking of cultural artefacts and the absence of clear policy guidance on the use of artificial intelligence in this area.

Through this approach, the article offers a framework for critical reflection on the integration of artificial intelligence into the mechanisms for safeguarding cultural heritage, emphasizing the need for cooperation between cultural institutions, legal authorities and digital platforms.

Digital mechanisms for trafficking cultural goods

Contemporary society is shaped by technology and widespread internet access, factors that have profoundly reshaped social, economic and cultural structures. Information systems are ubiquitous and influence every dimension of daily life, while the rapid circulation of information has transformed the modern world into a knowledge society, often referred to as an information society (*Library, Information and Society*, 2024).

The Internet has become the main driver of the information society, providing rapid access to resources and removing traditional communication barriers. Its ease of use and global reach have made it indispensable, leading to an exponential increase in the number of users.

This evolution has redefined social and economic relations, profoundly influencing the power structure, education and decision-making processes, thus creating a new way of organizing and functioning in the modern world (Băjenescu, 2006).

Technological advancements have radically transformed the mechanisms of illicit cultural artefact trafficking and have facilitated the rapid and anonymous distribution of looted or stolen cultural goods. In addition, the Internet offers global access, secure platforms for transactions and encrypted communication channels, which make it

difficult to monitor, prevent and combat illicit practices with antiquities (Amineddoleh, 2015).

As the above being mentioned, a significant side effect of technological progress is the adaptation of illicit trafficking with cultural objects to the global digital infrastructure. This type of transnational crime does not only affect directly the universal cultural heritage, but has also consolidated itself as a financing mechanism for organized crime networks and terrorist groups (UNESCO, 2025).

According to the specialized literature, illicit trafficking and trade with cultural artefacts represents one of the most profitable black markets worldwide, generating annual revenues of billions of dollars and involving a complex network of actors and transactions that are difficult to trace (Willett, 2016).

Illicit trafficking of cultural goods encompasses the export or unlawful transfer of artefacts in contravention to national or international laws. Such activities are frequently motivated by commercial gain or exploited to finance criminal networks and terrorist organizations, underscoring the critical link between cultural crimes and global security concerns (UNESCO, n.d.).

In the context of technological development, social networks have become basic channels for illegal transactions involving cultural artefacts. Traffickers exploit the facilities offered by these media – anonymity, encrypted communication, global visibility – to promote, negotiate and sell cultural goods to potential buyers, in a framework lacking institutional supervision and clear regulation (Mashberg, 2020).

In the specialized literature, the use of the Internet by terrorist groups for propaganda, recruitment, planning attacks or money laundering has been intensively documented and analysed. However, the dimension aimed at obtaining financial resources through digital trafficking and trade with cultural artefacts remains insufficiently investigated, despite the increasing evidence regarding the use of digital infrastructure to monetize cultural heritage stolen from conflict zones (Todorovic and Trifunovic, 2020).

This research gap leaves in the shadows an emerging financing mechanism that eludes the traditional framework for investigating

terrorism and organized crime, but which benefits from the same cybernetic advantages: anonymity, decentralization and lack of regulation.

In the online environment, the illicit trafficking of cultural artefacts represents a continuation of traditional smuggling, adapted to the digital space, where criminal networks exploit technological vulnerabilities to finance their activities.

Online platforms provide distribution networks with the ability to expand rapidly and access the international market with ease, while at the same time reducing the risks associated with the physical transportation of artefacts. Within these networks, information about cultural goods is often compartmentalized, anonymized and disguised, allowing direct contact with buyers and transactions with minimal risk of exposure (Suárez-Mansilla, 2018).

A relevant example of the cyber dimension of the illicit trafficking and trade of antiquities is the use of the social network Facebook as a tool for promoting, selling and even organizing criminal activities. While Facebook was initially a simple means of uploading and sharing photos and videos, the platform now offers advanced features such as live streaming, video chat and encrypted messaging, which facilitate illegal transactions and communications between traffickers (Azm and Paul, 2018).

Although the first forms of digital trafficking through social networks were observed ever since 2011, the phenomenon gained significant breadth after 2014, following the intensification of the actions of the Islamic State, which orchestrated the systematic looting of archaeological sites in Iraq and Syria. The Islamic State turned cultural heritage into a dual resource: a source of funding and a tool for propaganda. This strategy marked the beginning of a new era in terrorist financing, driven by the illicit trafficking and trade of antiquities (Azm and Paul, 2018).

Thus, Facebook has become a space for interconnection between local looters located in different conflict zones, such as: Libya, Yemen, Syria, Iraq, and potential buyers from all over the world. Through its own algorithms, the platform facilitates not only the rapid promotion of cultural goods, but also their authentication through crowdsourcing and the efficient dissemination of illicit information. In this way, this platform

has been transformed into a digital space conducive to the rapid dissemination of illicit information and the facilitation of commercial contacts between actors involved in the trafficking of artifacts (Azm and Paul, 2023).

A relevant example is the ATHAR project (Antiquities Tracking and Heritage Anthropology Research Project), which identified ninety-five Facebook groups involved in the illicit trafficking of cultural artefacts. These groups operated under three levels of confidentiality: public, closed and secret, of which twenty-eight were public, sixty-five closed and two secret. This highlights the way these networks operate in an environment that is partially or completely opaque (Azm and Paul, 2019).

The closed structure of these groups facilitated the operation and expansion of illicit activities, while also allowing for their rigorous control. In some cases, group administrators required potential members to pay a search fee, the so-called *khums tax*. This fee system, initially established by the Islamic State, indicates both a form of self-financing as well as a continuity of the ideological and logistical network that, although physically destructed, has transformed and adapted itself to the digital environment (Azm and Paul, 2019).

Although Facebook has banned the sale of looted cultural goods, the enforcement of these policies has been fragmented and ineffective, being left largely to users, who could report suspicious content. In the absence of a specialized moderation team capable of assessing the provenance and authenticity of cultural artefacts, these notifications have not had a substantial impact.

Furthermore, following an investigation by the BBC and public pressure from experts such as Professor Al-Azm and his colleagues, Facebook decided to remove forty-nine groups involved in the illicit trafficking of antiquities, which highlighted another serious vulnerability, namely the lack of a protocol for preserving and sharing digital data (Swann, 2019). By directly deleting the content, valuable evidence for official investigations was lost, which undermines international efforts to dismantle the networks involved (Zraick, 2019).

In this context, in the absence of clear protocols for sharing data with the competent authorities, social networks become a space of digital

impunity and the responsibility of digital platforms is minimized, with traffickers benefiting from reduced visibility and minimal operational risks (The European Institute for International Relations, 2022).

Although online platforms have added cultural artefacts to the list of prohibited items alongside with drugs and weapons, this measure remains ineffective without clear mechanisms for monitoring and compliance (Azm and Paul, 2023). The lack of cultural expertise within moderation teams and the absence of systematic cooperation with law enforcement hinder the effective implementation of these rules, allowing the illicit trade to persist online.

In the digital environment antiquities traffickers employ advanced technique to conceal their identity and avoid detection. These include falsifying photo metadata, using crypto currencies for anonymous payments and employing proxies or VPNs to mask their location.

Photo metadata contains information about the date, time and location where the photograph was taken. These data, known as EXIF (Exchangeable Image File Format) can be modified and/or removed by traffickers to conceal the origin of artefacts and prevent the identification of their actual location. Manipulating metadata hinders investigations and makes it difficult to trace the path of cultural objects from their source to the market (Awati and Sheldon, 2024).

The manipulation of photo metadata in not explicitly addressed to in the literature on illicit trafficking of cultural artefacts, however it is a well-documented practice in other illicit activities, such as human trafficking (United Nations Office on Drugs and Crime [UNDOC], n.d.).

This gap underscores the significant challenges faced by authorities in detecting and combating this concealment method employed by traffickers to facilitate the illicit trade of cultural artefacts.

As for crypto currencies, they offer a high degree of anonymity to illicit transactions involving cultural artefacts, making them a favourite choice for traffickers due to the difficulty of monitoring such payments. They are used by both buyers and sellers because they (Sargent et al., 2020):

- guarantee transaction confidentiality and prevent the tracking of financial flows,
- eliminate the involvement of financial institutions that might report suspicious transactions,

- facilitate fast and unrestricted cross-border fund transfers.

Traffickers take advantage of digital tools that provide anonymity in the online environment. In the online trafficking of cultural goods, VPN (Virtual Private Networks) networks and proxy servers are frequently used to conceal the identity and true location of those involved (Fraudlogix, n.d.).

These tools mask the IP address, which significantly hinders the efforts of authorities to identify and locate suspects. Although the specialized literature does not explicitly address to the use of these technologies in the trade of cultural artefacts, their application is well-documented in other illegal activities due to high level of confidentiality they provide (Harrison, 2018).

Similar to practices in human trafficking and terrorist financing, these mechanisms are likely used in this context to shield criminal networks and terrorist groups from detection and prosecution (Bing, 2016).

The escalation of digital tactics employed by criminal networks, from metadata manipulation to identity concealment through VPNs and crypto currencies, highlights the limitations of traditional investigative methods. This situation requires the development of innovative solutions capable of adapting to the dynamics of the cyberspace. Artificial intelligence is emerging as one of the most effective solutions for identifying the illicit trafficking of cultural artefacts.

Artificial Intelligence – a mechanism to prevent illicit trafficking

Relying on the points discussed above, we consider the use of artificial intelligence (AI) in combating the illicit trafficking of cultural artefacts to represent a significant advancement in detecting, preventing and countering of illegal activities aimed at generating financial resources for terrorist groups.

This technology enables the rapid and efficient analysis of large amounts of data, facilitating the identification of suspicious cultural objects and the continuous monitoring of illicit activities conducted in the online environment (Abate et al., 2023).

Artificial intelligence (AI) can be used in several ways to prevent and combat illicit trafficking with antiquities, including:

The automatic identification of suspicious cultural artefacts is carried out by AI systems through the use of visual recognition, comparative analysis and metadata analysis, each method contributing to the verification of the artefacts authenticity and provenance.

Visual recognition and comparative analysis are complementary in the identification of suspicious cultural artefacts. Visual recognition extracts the distinctive features of artefacts, such as shape, texture, ornamentation and inscriptions, and converts them into digital profiles (Patias and Georgiadis, 2023)

Deep learning algorithms, particularly convolutional neural networks (CNN) analyse these features to compare the cultural objects with international database, such as those maintained by INTERPOL or UNESCO, identifying discrepancies that may indicate forgery or illicit provenance (Winterbottom et al., 2022).

Comparative analysis utilizes digital profiles generated through visual recognition to evaluate suspicious objects against authentic cultural artefacts in international databases. By comparing visual features, such as shape, texture, colour and inscriptions, the system identifies similarities that confirm authenticity, as well as subtle discrepancies that may indicate forgery or illicit provenance.

In parallel, the analysis of associated metadata provides additional information that contributes to verifying the credibility of the artefact. By correlating visual data with metadata, comparative analysis becomes an effective tool for the rapid identification of suspicious cultural objects and for supporting law enforcement agencies in their efforts to safeguard cultural heritage.

Monitoring online sales and social media has become essential in preventing the illicit trafficking of cultural artefacts. E-commerce platforms and social networks are increasingly used for trading such items, providing traffickers with the ability to communicate anonymously and conceal their identity, which significantly complicates the detection of illegal transactions (Swann, 2020).

To counter these practices, artificial intelligence-based systems employ natural language processing (NPL) techniques to analyse object

descriptions, messages and comments associated with online posts (Ferro et al., 2025).

The algorithms identify terms, ambiguous expression, or coded language used in illicit trade, such as indirect references to archaeological artefacts, geographic locations, or historical periods. In addition, NLP detects semantic anomalies, including discrepancies between descriptions and images or the absence of provenance information.

This textual analysis is combined with visual recognition of images to correlate the language used with the characteristics of the cultural objects. In parallel, the analysis of associated metadata enables the identification of locations, transaction histories and connections between suspicious accounts (Ünver, 2023).

By integrating these methods, artificial intelligence systems can rapidly detect suspicious accounts, communication patterns and transactional networks, thereby supporting authorities in investigating and preventing illicit trafficking. This combined approach provides a comprehensive and effective tool for protecting cultural heritage (Abate et al., 2023).

The analysis and mapping of criminal networks represent an advanced tool employed by artificial intelligence (AI) to combat the illicit trafficking of cultural artefacts. By collecting and correlating data from suspicious transactions, geographic locations, online interactions and users' profiles, artificial intelligence can construct dynamic maps of criminal networks, highlighting connections between actors who appear to be independent (Adán and Loureiro, 2023).

By using Social Network Analysis (SNA) and Machine Learning (ML) algorithms, behavioural patterns that indicate illegal activities can be identified. These algorithms monitor the frequency of specific terms or expressions, activity times and days, encrypted payment methods and unexpected price fluctuations (Giovanelli and Traviglia, 2024).

By detecting these patterns suspicious accounts or transactions can be highlighted, enabling authorities to focus on high-risk elements and anticipate traffickers' strategies.

Furthermore, artificial intelligence applies anomaly detection techniques to identify hidden connections between accounts and

transactions by analysing IP addresses, transaction histories and users' interactions (Komenchuk, 2025). This information enables the reconstruction of criminal network structures, highlighting illicit flows and identifying central nodes – the individuals or entities that play a key role in coordinating and organizing the cultural trafficking (Malinverni, et al., 2024).

In view of the above, we recall the European project SIGNIFICANCE, which employs machine learning algorithms to monitor suspicious transactions on the Internet and Dark Web. The importance of this projects lies not only in its technical capacity but also in its ability to demonstrate how AI technologies can support authorities in anticipating and mapping criminal networks. At the same time, it highlights the necessity of institutional collaboration and the development of interoperable databases to enhance the effectiveness of such systems (Abate et al., 2022).

The analysis of the specialized literature highlights the fact that the efficiency of these technological tools is conditioned by certain essential factors, among which we mention: access to extensive, updated and interoperable databases, as well as international collaboration between law enforcement authorities, cultural institutions and international organizations.

A crucial step in enhancing the effectiveness of artificial intelligence in combating the illicit trafficking of cultural artefacts is the integration with international databases, such as those maintained by UNESCO, INTERPOL or digital museum collections.

By connecting artificial intelligence systems to international databases, the authenticity of cultural artefacts circulating online can be verified in real time. When a cultural object is posted on a digital platform, visual recognition algorithms analyse its physical characteristics, such as shape, dimensions, texture, decorations and inscriptions, and convert them into digital profiles (Patias and Georgiadis, 2023).

Furthermore, the metadata associated with images and the descriptions of artefacts are automatically cross-referenced with information from official databases UNESCO, INTERPOL, or museum collections. Any discrepancy, such as unverified provenance, incorrect dating or differences in dimensions and visual characteristics, is detected

immediately. This automated correlation enables the rapid identification of potential forgeries, trafficked cultural objects or suspicious transactions, providing authorities with an effective means to prevent and combat the illicit trafficking of cultural goods (Daskalakis et al., 2024).

This continuous analysis allows AI systems to alert authorities immediately when suspicious artefacts appear in the digital environment. This way, monitoring shifts from a reactive process to a proactive process. Moreover, real-time verification facilitates the rapid correlation of cultural objects with transactions, accounts and criminal networks involved, providing a comprehensive picture of illicit activities (Daskalakis et al., 2024).

Thus, through integration with international databases and the utilization of the aforementioned technologies, artificial intelligence emerges as a strategic tool capable of optimizing both prevention and intervention in the protection of international cultural heritage.

Challenges and limitations in the use Ai for preventing and combating the digital trafficking in illicit artefacts

The integration of artificial intelligence into the prevention and combat of illicit trafficking of cultural artefacts involves a series of technical, ethical and legal challenges and limitations, which require careful analysis to evaluate the effectiveness and feasibility of these technologies.

From a technical perspective, the integration of artificial intelligence technologies into the processes of identifying, authenticating and monitoring cultural goods trafficked online shows considerable potential promise (Zhan, 2025). Nevertheless, the effectiveness of these solutions depends directly on the quality of the data, the stability of the algorithms and their capacity to operate in complex digital environments. Without a careful understanding of these challenges, prevention strategies risk losing their effectiveness or even generating unintended consequences.

A primary challenge in applying artificial intelligence to the prevention of digital trafficking of illicit cultural artefacts is related to the limited availability and low quality of data. Machine learning models, particularly those based on deep learning, require substantial volumes

of visual and contextual data to recognize patterns, distinguish authentic cultural artefacts from forgeries and identify subtle indications of illicit provenance (Winterbottom et.al. 2022).

In the field of cultural heritage, data are often fragmented (for example: museum collections cover only a fraction of the relevant cultural assets, photographs vary in resolution and quality, and metadata concerning provenance or conservation status are frequently incomplete or inconsistent). This fragmentation leads to reduced sensitivity and increases the error rate (Foka et. al., 2025).

It is worth noting that most existing datasets include artefacts from well-documented historical periods or civilizations, while cultural objects associated with lesser-known or insufficiently research civilizations are underrepresented. This unequal distribution of data can introduce structural bias into artificial intelligence algorithms, leading them to more easily recognize cultural objects derived from well-documented civilizations, while rare or less-known artefacts are identified with lower accuracy (Liu et al., 2025).

Thus, algorithmic biases in artificial intelligence systems are configured as follows: models trained on limited, unbalanced or poorly labelled datasets tend to reproduce distortions of the available information (Zhan, 2025). These algorithmic biases can be amplified by the way data is processed: inconsistent labelling, lack of terminological consensus among institutions or the arbitrary removal of less clear records. This leads to systematic errors in the learning process (Foka et. al., 2025).

Deep-learning-based AI models, such as convolutional neural networks, which have been predominantly trained on a particular class of cultural artefacts or on images acquired under ideal conditions, tend to underperform when they encounter artefacts originating from different historical periods, styles, acquisition angles, illumination conditions or states of degradation (Antun et al., 2020).

The scholarly literature underscores the challenges of metadata inconsistency and insufficiency associated with cultural artefacts. Core descriptors such as geographical provenance, chronology, materials or conservation status are frequently incomplete or recorded in heterogeneous schemas, which complicates metadata interoperability

and hinders the correlation of information on provenance, authenticity and transaction history (Liu et al., 2025).

The absence of unified standards for structuring and harmonizing metadata terminology leads to a loss of accuracy and stability in artificial intelligence models, thereby limiting their capacity to effectively support the prevention and combat of illicit trafficking in cultural property.

The issue of data scarcity encompasses dimensions related to the quality, consistency, diversity and accessibility of information. In the absence of a coordinated strategy for data collection, data cleaning and harmonization, the potential of artificial intelligence in preventing and combating the digital trafficking of illicit cultural property is undermined and the results risk being partial or discriminatory.

Another challenge in applying artificial intelligence to the prevention of digital trafficking in cultural heritage objects is data confidentiality. Machine learning algorithms rely on access to a wide range information, such as transaction records, data concerning the location of artefacts or the individuals involved, and images extracted from online platforms in order to rapidly detect suspicious cultural property (Zhan, 2025). However, the processing of such data risks relates both to the privacy of the individuals involved and to the management of cultural sensitivity associated with certain cultural assets.

The large-scale processing of data entails the risk of disclosure and misuse of personal data by malicious individuals or entities, as well as the exposure of sensitive information concerning the provenance and location of cultural heritage objects (Mademlis, 2024).

The excessive collection of data about users or legitimate sellers may violate data protection legislation, such as the General Data Protection Regulation (GDPR), and may undermine the trust of stakeholders involved in the management of cultural heritage (Zhan, 2025).

The protection of personal data is essential; however, overly restrictive or fragmented regulations may limit the access of artificial intelligence systems to the information necessary for detecting and preventing digital trafficking of cultural objects. At the same time, the lack of a coherent approach at the international level can generate legal uncertainty and additional costs for organizations developing solutions

dedicated to the protection of cultural heritage, thereby discouraging their large-scale implementation (Zhan, 2025).

These difficulties highlight the importance of harmonizing confidentiality requirements with the need for access to relevant data for artificial intelligence systems. Thus, a clear and coherent regulatory framework at both national and international levels can support the responsible processing of information, ensuring respect for fundamental rights as well as the effectiveness of technological solutions.

To understand the legal challenges concerning the use of artificial intelligence in combating the digital trafficking of artefacts, it is necessary to examine the evolution of the international legislative framework.

Since 2015, the systematic destruction and looting in Iraq and Syria have highlighted the link between cultural crimes and the financing of terrorism (Terlinden, 2023). Consequently, the international community has adopted legislative measures and global policies to prevent and combat the destruction, looting and trafficking of cultural property, thereby elevating the protection of cultural heritage to a strategic security objective (United Nations Office on Drugs and Crime [UNDOC], 2016).

Although numerous journalistic investigations, specialist reports and academic studies highlight the fact that cultural artefacts are actively promoted, sold and traded on digital platforms – including through social networks, encrypted applications and online marketplaces – the digital component of trafficking with cultural goods continues to be ignored in the regulatory context.

Following the analysis of the international legislative framework, the European Union's Action Plan against the trafficking of cultural goods, adopted in 2022, stands out as it explicitly recognizes the potential of emerging technologies, such as artificial intelligence and aerial surveillance, in identifying and preventing the illicit trade in cultural artefacts (European Commission, 2022).

Given that this is the only legislative document that refers to the potential of artificial intelligence, without providing a concrete implementation framework for the European Union member states, we aim to identify and evaluate how global policies address to the role of artificial intelligence in the prevention and combat of digital trafficking of illicit cultural property.

At the international level, a series of policies aimed at regulating and applying artificial intelligence have been adopted and implemented. In 2019, the Organization for Economic Cooperation and Development (OECD) launched the Principles on Artificial Intelligence, the first major intergovernmental set of major guidelines dedicated to the governance of this technology (Russo; Oder, 2023). These principles, of a recommendatory nature (soft law), promote five essential directions: inclusive and sustainable growth, respect for human rights and democratic values, transparency and explainability, robustness and security, as well as accountability (OECD, n.d.).

With regard to the protection of cultural heritage, these principles do not directly refer the fight against illicit trafficking of artefacts carried out online. These can be interpreted as a foundation for the ethical use of AI technologies in the process of verifying the provenance and authenticity of cultural objects.

Nevertheless, the absence of practical mechanisms and of an approach specific to the cultural field makes it difficult to directly apply the principles in the domain of cultural heritage protection.

In 2021, UNESCO adopted a global recommendation establishing a universal ethical framework for the development and use of artificial intelligence. The document promotes values such as fairness, transparency, respect for human rights and cultural diversity (UNESCO, 2023).

From the perspective of cultural heritage protection, these principles can guide the implementation of AI applications aimed at artefacts or the monitoring of suspicious digital transactions.

However, the recommendation remains a soft law instrument, lacking legally binding force and without providing concrete tools for application in the context of digital artefacts trafficking, which limits its immediate impact.

In 2024, the AI Act was adopted as the European Union's first legally binding legislative framework regulating the use of artificial intelligence. Its purpose is to protect fundamental rights, ensure transparency and accountability and strengthen trust in emerging technologies (European Commission, n.d.).

Although the Act does not directly address the cultural sector or the issue of digital trafficking of artefacts, the principles and standards it

establishes for high-risk AI systems can serve as a significant regulatory benchmark.

This is explained by the fact that the AI Act introduces clear requirements for transparency, auditability and security, establishes accountability obligations for developers and users and endures the harmonization of regulations across the European Union (European Commission, n.d.).

All of these elements can be extrapolated to the field of cultural heritage protection, providing a general legal framework that could underpin sectorial policies dedicated to the prevention and combat of digital trafficking of illicit cultural goods.

These global policies on artificial intelligence provide an increasingly clear framework for the responsible use of this technology in the prevention and combat of digital trafficking of illicit cultural artefacts. Nevertheless, their application remains challenging, as certain legal systems do not accept algorithm-generated data as valid evidence unless accompanied by transparency and auditability (Fair Trials, 2022). This highlights the need to develop transparent and auditable AI solutions that are compatible with the evidentiary requirements of legal systems.

This evidentiary obstacle is represented by the normative gap resulting from the absence of international legislation governing digital trafficking of illicit cultural artefacts. Furthermore, global policies on artificial intelligence governance do not provide support for the use of this technology in the prevention and combat trade of illicit cultural property. These gaps reduce the effectiveness of a coordinated response and highlight the need for an integrated legislative framework that harmonizes the rules concerning cultural heritage with those dedicated to innovative technologies.

Possible solution for improving the prevention and combat of digital trafficking in illicit antiquities

The review and analysis of technical, ethical and legal challenges have highlighted that, in the absence of corrective measures, the potential of artificial intelligence in preventing and combating digital trafficking of illicit cultural objects risks to remain fragmented and insufficiently harnessed. Nevertheless, these limitations outline future directions

for the development of innovative solutions capable of combining technological efficiency that complies with legal and ethical standards.

Federated learning constitutes an innovative approach to overcoming challenges related to data privacy and data accessibility through the collaborative training of artificial intelligence models. This mechanism enables algorithms to be trained on distributed datasets across multiple institutions, such as museums, online platforms, customs agencies and law enforcement authorities, without raw data being transferred or exposed to security risks (Gong et al., 2024).

Thus, a balance is established between the need to access substantial volumes of information and the requirement to comply with data privacy regulations. Moreover, through the decentralized aggregation of information, artificial intelligence systems become more robust and less dependent on the idiosyncrasies of a single dataset, thereby mitigating the risk of algorithmic bias (Huang et al., 2024).

Federate learning addresses the challenges of privacy-preserving data protection while enabling broader access to relevant datasets. Nevertheless, its applicability remains limited in analytical contexts that require context-dependent semantic interpretation of cultural, legal and historical dimensions.

Therefore, the actual effectiveness of technological tools emerges when they are complemented by the expertise and discernment of domain specialists, a synergy that can strengthen efforts to prevent and combat digital trafficking of illicit cultural property. To ensure technical accuracy as well as the probative validation of results, collaboration between humans and artificial intelligence becomes indispensable. Although algorithms can detect subtle anomalies in metadata, suspicious transactions or cultural objects with uncertain provenance, only specialists can validate and correctly interpret these data and transform them into credible legal evidence (Adán and Loureiro, 2023).

The integration of automation with human expertise supplies a balanced framework of action, in which technology provides speed and the capacity to process large volumes of data, while specialists ensure rigorous interpretation and the prevention of errors and misuse of results. In the absence of such a partnership, risks increase considerably, either through excessive reliance on opaque algorithms or through the

significant slowdown of investigations conducted exclusively via manual verification (Abate et al., 2022).

Thus, a well-structured collaboration between humans and artificial intelligence enhances the effectiveness of detecting, preventing and combating digital trafficking of illicit cultural artefacts, while simultaneously providing safeguards for the observance of legal and ethical principles (Malinverni et al., 2024).

The development of specialized algorithms tailored to the specific characteristics of cultural artefacts represents another key factor in leveraging artificial intelligence for cultural heritage protection. General-purpose models, which are trained on large-scale datasets, fail to capture the subtle details associated with cultural artefacts (Kaldeli, 2023). This shortcoming leads to classification errors and generates confusion between authentic and falsified cultural objects.

Training algorithms on diversified and contextualized collections would enable more accurate recognition of cultural objects and a more precise differentiation between authentic artefacts and sophisticated forgeries (Malinverni et al., 2024).

At the same time, the integration of historical (Daskalakis et al., 2024) and legal metadata (such as provenance documentation, ownership history and applicable legal regime) into these modules would add a valuable evidentiary dimension (Kaldeli, 2023).

This way, the results generated by artificial intelligence would not be limited to mere visual classification but could be used as support in legal investigations and provenance verification processes. Such an approach would enhance the credibility and auditability of digital evidence, reinforcing its value in both legal and cultural contexts.

Conclusions

The findings of this study underscore the complexity and dynamism nature of digital crimes involving illicit cultural artefacts. While artificial intelligence has proven to be a valuable instrument for the monitoring and preventing of such cultural offenses, its potential is constrained by critical factors such as data incompleteness, information fragmentation and the ethical and legal dilemmas associated with data privacy.

This study also highlighted the existence of a regulatory gap: at present, the international legal framework does not directly regulate the cyber dimension of cultural trafficking, nor the application of emerging technologies in the prevention and combat of such illicit activities.

The prevention and combat of digital trafficking of illicit cultural artefacts cannot be addressed solely from a technological or legal perspective. Although algorithms and AI-based processes can handle large volumes of data with a speed unattainable by human experts, they cannot substitute for human judgment and the expertise required for the interpretation and validation of results.

Therefore, only through a solid partnership between human expertise and digital tools can both the efficiency of detection and the legal value of evidence be ensured.

In conclusion, a sustainable synergy should be made in which artificial intelligence is complemented by adapted ethical standards and public policies. Through such complementarity, artificial intelligence can fully realize its potential, becoming a strategic instrument in the fight against digital cultural crime.

References:

1. Abate, D., Benedetti, R., Amicone, E., Scopigno, R. (2022). "Significance: Stop illicit heritage trafficking with artificial intelligence." *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, 43*, pp. 729–736. https://doi.org/10.5194/isprs-archives-XLIII-B2-2022-729-2022.

2. Abate, D., Benedetti, R., Amicone, E., and Scopigno, R. (2023). "Artificial intelligence to fight illicit trafficking of cultural property." *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, 48*, pp. 3–10. https://doi.org/10.5194/isprs-archives-XLVIII-M-2-2023-3-2023

3. Adán A. G., Loureiro M. Á. F. (2023). "Ethical and Legal Risks of Algorithmic and AI Tools Developed to Fight Against Trafficking in Cultural Property in the RITHMS Project." *Proceedings XoveTIC*, pp. 343-349. https://rithms.eu/images/publications/Ethical%20and%20Legal%20Risks%20of%20Algorithmic%20and%20AI%20Tools%20Developed%20to%20Fight

%20Against%20Trafficking%20in%20Cultural%20Property%20in%20the%20RITHMS%20Project.pdf.

4. Al-Azm, A., Paul, K. A. (2018, August 14). "*How Facebook made it easier than ever to traffic Middle Eastern antiquities." World Politics Review*. https://www.worldpoliticsreview.com/how-facebook-made-it-easier-than-ever-to-traffic-middle-eastern-antiquities/?nsl_bypass_cache=a85de525c58c4f686ba0d46b74d0f934.

5. Al-Azm, A., & Paul, K. (2019). *Facebook's black market in antiquities: Trafficking, terrorism, and war crimes*. ATHAR Project. https://atharproject.org/wp-content/uploads/2019/06/ATHAR-FB-Report-June-2019-final.pdf.

6. Al-Azm, A., Paul, K. (2023). "Facebook's flawed plan to end antiquities trafficking." *Foreign Affairs*, 1–10.

7. Amineddoleh, L. A. (2015). "Cultural heritage vandalism and looting: The role of terrorist organizations, public institutions and private collections." *Santander Art and Culture Law Review, 2*(1), 27–62. https://doi.org/10.4467/2450050XSR.15.012.4510.

8. Antun, V., Renna, F., Poon, C., Adcock, B., Hansen, A. C. (2020). "On instabilities of deep learning in image reconstruction and the potential costs of AI." *Proceedings of the National Academy of Sciences*, 117(48), 30088-30095. https://doi.org/10.1073/pnas.1907377117.

9. Awati, R., Sheldon, R. (2024, October 17). *What is image metadata and how is it used?* TechTarget. https://www.techtarget.com/whatis/definition/image-metadata.

10. Băjenescu I. T. (2006). *Internetul, societatea informațională și societatea cunoașterii*. [*The Internet, the information society and the knowledge society*]. Bucharest: Matrix Rom.

11. Bing, C. (2016, July 21). *Report: Terrorists are big fans of VPNs*. FedScoop. https://fedscoop.com/isis-vpn-dark-web-flashpoint-2016/.

12. Daskalakis, E., Alexakis, T., Peppes, N., Demestichas, K., Adamopoulou, E. (2024). "A semantic engine for fighting cultural goods crime." *In Security informatics and law enforcement*, pp. 213-223. https://doi.org/10.1007/978-3-031-62083-6_17.

13. European Commission. (2022). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU action plan against trafficking in cultural goods* (COM(2022) 800 final). https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52022DC0800.

14. European Commission. (n.d.). *AI Act.* https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

15. Fair Trials. (2022). *Regulating artificial intelligence for use in criminal justice systems in the EU* (Report No. 7). https://www.fairtrials.org/app/uploads/2022/01/Regulating-Artificial-Intelligence-for-Use-in-Criminal-Justice- Systems-Fair-Trials.pdf.

16. Ferro, S., Giovanelli, R., Leeson, M., De Bernardin M., Traviglia A. (2025). "A novel NLP-driven approach for enriching artefact descriptions, provenance, and entities in cultural heritage." *Neural Computing and Applications, 37, 21275-21296*. https://doi.org/10.1007/s00521-025-11449-2.

17. Foka, A., Griffin, G., Pablo, D. O., Rajkowska, P., Badri, S. (2025). "Tracing the bias loop: AI, cultural heritage and bias-mitigating in practice." *AI & Society.* https://doi.org/10.1007/s00146-025-02349-z.

18. Fraudlogix, (n.d.). *IP Masking and VPN Usage: Understanding How Proxies Can Hide the True Location of a User or Device*. Fraudlogix. https://www.fraudlogix.com/blog/ip-masking-and-vpn-usage-understanding-how-proxies-can-hide-the-true-location-of-a-user-or-device/.

19. Giovanelli, R., Traviglia, A. (2024). "AIKoGAM: An Ai-driven Knowledge Graph of the Antiquities Market: Toward Automatised Methods to Identify Illicit Trafficking Networks." *Journal of Computer Applications in Archaeology, 7(1), 92-114*. https://journal.caa-international.org/articles/130/files/65a4fb5646957.pdf.

20. Gong, B., Mahsan, I. P., Xiao, J. (2024). "Federated learning-driven collaborative recommendation system for multi-modal art analysis and enhanced recommendations." *PeerJ Computer Science*, 10, e2405. https://doi.org/10.7717/peerj-cs.2405.

21. Harrison. S. (2018). *Evolving tech, evolving terror*. Center for Strategic & International Studies. https://www.csis.org/analysis/evolving-tech-evolving-terror.

22. Hill, V. C. (2016). "Killing a Culture: The International Destruction of Cultural Heritage in Iraq and Syria under International Law." *Georgia Journal of International and Comparative Law,* 45, pp. 191-220. https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2378&context=gjicl.

23. Huang, W., Ye, M., Shi, Z., Wan, G., Li, H., Du, B., Yang, Q. (2024). "Federated Learning for Generalization, Robustness, Fairness: A Suvey and benchmark." *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 46(12), pp. 9387-9406. https://doi.org/10.1109/tpami.2024.3418862.

24. Kaldeli, E. (2023, February 16). "Combining AI tools with human validation to enrich cultural heritage metadata." *Europeana Pro*. https://pro.europeana.eu/post/combining-ai-tools-with-human-validation-to-enrich-cultural-heritage-metadata.

25. Kersel, M. M., Gerstenblith, P. (n.d.). "Cultural heritage and security policy." *The University of Chicago Legal Forum.* https://legal-forum.uchicago.edu/print-archive/cultural-heritage-and-security-policy.

26. Library, Information and Society. (2024, February 5). *From information to knowledge society: What it means for the future.* LIS Academy. https://lis.academy/library-information-and-society/information-to-knowledge-society-future-impact/.

27. Liu. H., Yang, X., Frick, R. A., Steinebach. M. (2025). "Identification of Cultural Artefacts using Deep Learning." *Electronic Imaging*, 37(8), pp. 271-277. https://doi.org/10.2352/ei.2025.37.8.image-271.

28. Mademlis, I., Mancuso, M., Paternoster, C., Evangelatos, S., Finlay, E., Hughes, J., Radoglou-Grammatikis, P., Sarigiannidis, P., Stavropoulos, G., Votis, K., Papadopoulos, G. T. (2024). "The Invisible Arms Race: Digital trends in illicit goods trafficking and AI-Enabled responses*." IEEE Transactions on Technology and Society*, pp. 1-19, https://doi.org/10.1109/tts.2024.3514683.

29. Malinverni, E. S., Frontoni, E., Pierdicca, R., Troiano, L., & Bernardini, A. (2024). "SIGNIFICANCE: Deep learning-based platform to fight illicit trafficking of cultural heritage goods." *Scientific Reports, 14*, Article 1234, pp. 1–12. https://pubmed.ncbi.nlm.nih.gov/38956250/.

30. Mashberg, T. (2020, October 8). *Social networks: The new El Dorado for traffickers*. The UNESCO Courier. https://courier.unesco.org/en/articles/social-networks-new-el-dorado-traffickers.

31. OECD, (n.d.). *AI principles*. OECD. https://www.oecd.org/en/topics/ai-principles.html.

32. Patias, P., & Georgiadis, C. (2023). "Fighting Illicit Trafficking of Cultural Goods – The ENIGMA Project." *Remote Sensing*, *15*(10), pp. 1-14. https://doi.org/10.3390/rs15102579.

33. Russo, L., Oder, N. (2023, October 31). *How countries are implementing the OCDE Principles for Trustworthy AI*. OECD.AI. https://oecd.ai/en/wonk/national-policies-2.

34. Sargent, M., Marrone, J. V., Evans, A., Lilly, B., Nemeth, E., & Dalzell, S. (2020). *Tracking and disrupting the illicit antiquities trade with open-source data*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR2706.html.

35. Suárez-Mansilla, M. (2018). "Blood antiquities: A net acting in Spain helped to finance DAESH through illicit trafficking of cultural goods." *Art World Law Bulletin. Chronicles of Themis & Athenea, 4*, 1–32. https://artworldlaw.com/wp-content/uploads/2019/03/BloodAntiquities-IllicitTraffickingCulturalGoods-ConnectionTerrorism_MartaSMasilla.pdf.

36. Swann, S. (2019, March 17). *Antiquities looted in Syria and Iraq are sold on Facebook*. BBC News. https://www.bbc.com/news/world-middle-east-47628369.

37. Swann, S. (2020, June 23). *Facebook bans 'lot-to-order' antiquities trade.* BBC. https://www.bbc.com/news/world-middle-east-53140615.

38. Terlinden, M. (2023). *'Blood Antiquities': Funding the Islamic State with Art*. KU Leuven Institute for International Law & Leuven Centre for Global Governance Studies. https://ghum.kuleuven.be/ggs/wp236-marieterlinden-1.pdf#page=2.18.

39. The European Institute for International Relations. (2022, September 29). *How Facebook is involved in the illicit trade of cultural goods?* The European Institute for International Relations. https://www.eiir.eu/international-law/international-law-cases/how-facebook-is-involved-in-the-illicit-trade-of-cultural-goods/.

40. Todorovic, B., Trifunovic, D. (2020). "Prevention of (ab-)use of the internet for terrorist plotting and related purposes." *International Centre for Counter-Terrorism*, 594–619. https://icct.nl/sites/default/files/2023-01/Chapter-19-Handbook.pdf.

41. UNESCO. (n.d.). *About the fight against illicit trafficking of cultural property*. Retrieved June 15, 2025, from https://www.unesco.org/en/1970-convention.

42. UNESCO, (2023, May 16). *Recommendation on the Ethics of Artificial Intelligence*. UNESCO. https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence.

43. UNESCO. (2025, June 26). *Addressing Illicit Trafficking of Cultural Property in Digital Era*. UNESCO. https://www.unesco.org/en/articles/addressing-illicit-trafficking-cultural-property-digital-era.

44. United Nations Office on Drugs and Crime, (UNODC). (2016, September 12). *Protecting cultural heritage – An imperative for humanity.* https://www.unodc.org/documents/publications/SRIUN_Protecting_Cultural_Heritage_2016.09.12_LR.pdf.

45. United Nations Office on Drugs and Crime. (n.d.). *Using technology to prevent and combat trafficking in persons and smuggling of migrants*. SHERLOC. Retrieved June 15, 2025, from https://sherloc.unodc.org/cld/ar/education/tertiary/tip-and-som/module-14/key-issues/using-technology-to-prevent-and-combat-tip-and-som.html.

46. Ünver, A. (2023). *Emerging technologies and automated fact-ckecking: Tools, techniques and algorithms.* Cyber Governance & Digital Democracy Programme. https://edam.org.tr/Uploads/Yukleme_Resim/pdf-28-08-2023-23-40-14.pdf#page=2.11.

47. Willett, H. D. (2016). Ill-gotten gains: A response to the Islamic State's profits from the illicit antiquities market. *Arizona Law Review, 58*(3), 831–865. https://arizonalawreview.org/pdf/58-3/58arizlrev831.pdf.

48. Winterbottom, T., Leone, A., Al Moubayed, N. (2022). "A deep learning approach to fight illicit trafficking of antiquities using artefact instance classification." *Scientific Reports*, 12(1), 1-12. https://doi.org/10.1038/s41598-022-15965-2.

49. Zhan, X. (2025). "Artificial intelligence in the cultural industry: Applications and challenges." *Innovation in Science and Technology*, 4(1), 62-68. https://doi.org/10.56397/ist.2025.01.06.

50. Zraick, K. (2019, May 9). *Now for sale on Facebook: Looted Middle Eastern antiquities*. The New York Times. https://www.nytimes.com/2019/05/09/arts/facebook-antiquities-syria-iraq.html.

WAYS AND METHODS TO OPTIMIZE THE SELECTION PROCESS OF PERSONNEL PARTICIPATING IN MULTINATIONAL OPERATIONS

Alice-Claudiţa MANDEŞ*

Abstract:
Given Romania's participation in multinational operations under the auspices of the United Nations and the leadership of international security organizations such as the North Atlantic Treaty Organization and the European Union, in this article we have addressed the issue of optimizing the selection process of personnel participating in such military actions, which, in our opinion, is not only a necessity, but also a functional reality that influences the way the entire process is organized. The purpose of this article is to highlight a series of aspects that influence the management, planning and selection of military personnel participating in multinational operations outside the country. In the study conducted, we used the SWOT analysis (Strengths, Weaknesses, Opportunities and Threats) as a research method, to identify the normative acts that should be modified at the level of the military institution, to assess the impact of these changes on the selection process of military personnel for participation in multinational operations. Through the research conducted, we analyzed the extent to which the existing regulatory framework in the analyzed field ensures permanent adaptation to the realities of the new geopolitical and geostrategic environment, respectively the way in which the management structures of the personnel in the Romanian army manage to manage the legislative changes specific to this field.

Keywords*: NATO; EU; multinational operations; efficiency; personnel management; selection process; Romanian Army.*

Introduction

The accession and subsequent integration of our country, at different times, into Euro-Atlantic security organizations, such as the North Atlantic Treaty Organization (NATO) and the European Union

* Major PhD candidate, Romanian Joint Force Command. Military Sciences and Intelligence Field National Defense University "Carol I" Bucharest, Romania, email: mandesclaudita@gmail.com

(EU), represents, in the opinion of many political-military analysts, a natural consequence of the social, economic, human, material and financial efforts of Romania as a state and of the military institution as an organization to correctly address some of the challenges of the 1990s and later, of the first years of the 21st century, such as the multinational operations carried out under the aegis of two other international security organizations, with regional and global coverage, the Organization for Security and Cooperation in Europe (OSCE) and the United Nations (UN).

Romania's acceptance into NATO and the EU represented, in our opinion, a combined result of the reform and transformation processes of public institutions in our country, including the military institution. Thus, the participation of the staff and force structures of our country in multinational operations such as those in Somalia, the Republic of Moldova, Angola, Congo, the post-Yugoslav region, Albania, Iraq and Afghanistan, Mali, the Central African Republic, to name just a few, led to the creation of the conditions for acceptance and, subsequently, integration of our country into NATO and the EU, respectively, for the recognition of the professionalism of the Romanian military alongside those from the member states of the aforementioned organizations. (Neag, 2004, p. 1).

Existing legal framework

Participation in multinational operations, led by the UN, OSCE, NATO or EU, before and after our country's accession to the last two international security organizations was accompanied by a whole series of challenges, of a diplomatic, economic, financial, military and human nature. This type of involvement has always required a deep analysis of the existing geopolitical and strategic environment, of the security climate in the countries where the Romanian Army's force structures were deployed and, last but not least, repeated attempts in terms of organizational structure, endowment with military equipment and technology, allocation of considerable material and financial resources that aimed at the need to adapt to international military realities and to the implications identified in all areas of social life.

Firstly, the involvement of the Romanian army's force structures imposed a series of legislative changes at the military institution level, allowing them not only to take part in various military actions but also to

execute a wider range of operations, in cooperation with large units and units belonging to other states contributing troops (Alexandrescu, Duţu, 2007, pp. 15-16). Thus, the selection process of the military participating in the military operations, mentioned above, underwent a series of changes that primarily concerned, in addition to expressing volunteerism, a series of theoretical and practical knowledge, high-level mental and physical skills and, very importantly, an appropriate level of knowledge of one of the international languages of communication, with a predilection for English.

Secondly, depending on the country of deployment, the selection process also considered a component that targeted the standard operating procedures in the mission area, the realities of the deployment area, the risks and threats to which the participating soldiers could be exposed, on a case-by-case basis.

Although subject to normative regulations and habits formed over time, most of the time resistant to change, the selection process has become more efficient, with the passing of the years, with the gradual integration of our country into NATO and the EU, but also based on the experience gained in multinational operations by the Romanian military. A quick evaluation of such a selection process highlights both for the military participants (together with the structures they are part of) in multinational operations, and for the staff personnel who occupy various positions in multinational commands, five important tests, of which we mention: the English language test, the physical fitness level test, the psychological test, the theoretical (and practical) knowledge test, respectively the medical visit, the last stage that certifies the level of health and allows those participating in the selection to fulfill the missions received in optimal conditions.

For those who have taken part in such a selection process, whether they were tested or were part of those who organized and led the process itself, there are already known situations in which, after passing tests, such as those of knowledge of the English language (ALCPT test[1]), physical fitness and psychological testing, some of the candidates remaining in the race were either poorly prepared for the specifics of

[1] American Language Course Placement Test – an English language test designed to measure English ability levels through listening and reading.

the position, or did not know the foreign language well enough. Subsequently, the medical examination, the last of the tests (placed at the end, somehow for financial reasons, not always understandable) led to unsatisfactory results in terms of the number of soldiers admitted. Functions such as those in the legal, financial, medical, psychological fields were always difficult to fill by the candidates registered for the selection competition, perhaps also from the perspective of a need for fewer functions in the Romanian Armed Forces and less physically demanding ones that would allow them to easily pass the physical tests, most of the time, these tests being difficult trials for the participants to overcome. Thus, completing the selection process was and we still consider it to be a "burden" for those involved, given that for the recruitment of not very numerous structures, with a specific and special destination, such as those of the Operational Mentoring and Liaison Teams or the National Support Element, several selection sessions are carried out, in order to fully recruit these units.

In some cases, for objective selection reasons, some of these subunits went to the theaters of operations without being fully assigned. Although such situations have happened and will probably happen again, and although at the level of personnel structures such events accumulate that go from the stage of identified lesson to that of learned lesson (Pînzariu and Mocanu, 2016, pp. 70-71), legislative amendments that would ensure a high efficiency of the selection process are delayed, and in some cases, debates on this topic are even very little accepted.

Given that the process of attracting human resources to the Romanian Army is quite difficult (Alexandrescu and Duțu, 2007, p. 21), which does not always have as its main causes the lack of interest of the population of our country, the low degree of popularization of this process, the salary level (which has nevertheless been increasing in recent times), causes of a demographic nature or the nature of the selection pools existing in our country, we consider that optimizing the selection process for participation in multinational operations under the leadership of NATO and the EU is gaining much greater importance than some or other of the current military decision-makers want to accept. In this situation, we consider it necessary to review the entire selection process for participation in multinational operations to ensure a complete level of recruitment, as far as possible only with soldiers from

the structures nominated to participate (in singular cases with personnel from other structures) as well as staff personnel, who are to fill non-permanent positions within regional commands.

Scientific research methodology

The purpose of the research conducted in the field of human resources management was to identify the normative provisions that should be made, in order to ensure an increased level of efficiency in the selection process, given that both military structures and staff personnel from the Romanian army can participate, under the existing legislative framework, in an extensive range of operations conducted under the leadership of NATO and the EU, respectively within coalitions of forces, in some situations. From this perspective, participation in this type of operations brings important benefits to the army and our country through the continuous contribution to the efforts of the international community to ensure peace and security at a global level.

In the approach taken, we considered, in addition to the legislative provisions found in various laws, regulations, orders and instructions issued at the level of the Ministry of National Defense, a series of scientific references of high value (modern approaches, theories, reports, etc.) in the field of human resources management, on the basis of which we conducted this research.

Thus, we analyzed a series of scientific research papers, such as: the paper prepared by Alexandrescu, Grigore, Petre, Duțu, entitled *Optimization of the regeneration of the Romanian Army structures engaged in military actions outside the national territory*, 2007; the article prepared by Grigoraș, Răzvan, entitled *Prospective scientific methods in national security*, 2022; the article prepared by Ivorschi, Rodica*, SWOT analysis – a managerial tool for making the activity more efficient*, 2012; the article written by Lungulescu, Marilen, Alexandru, Adomnicăi, *Human resources in the Romanian Army, on the path of interoperability with similar structures from the armies of NATO member states*, 2012; the article by Palaghia, Mihai, *Principles and content of the force generation and regeneration system*, 2004; the material prepared by Neag, Mihai, *Present and perspectives regarding Romania's participation in NATO actions*, in Journal of the Academy of Land Forces, no 1, 2004; the study prepared by Pînzariu, Sorin, Bixi-Pompiliu, Mocanu, "Logistics Guide for Theaters of

Operations", 2016 or the article written by Stoica, Viorel, "Force Reserve and the Mechanism for Completing Losses in Military Actions", in 2015. At the same time, we analyzed a series of legislative provisions, presented in the bibliography, laws, GEO, ministerial orders, doctrines, and strategies, orders prepared at the level of the Chief of the Defense Staff or the heads of the armed forces categories.

The research objectives aimed, firstly, to identify the elements of novelty, at an international level, regarding the process of selecting human resources for participation in multinational operations and, secondly, to determine the overlapping elements regarding the tests administered for the actual selection with the tests that each soldier goes through, through the training process, within the units to which the soldiers belong. In this regard, we took into account the answers to research questions, such as: What are the elements of novelty identified at an international level? What are the legislative changes that need to be made to increase the efficiency of the selection process? Last but not least, we sought answers to the question: What are the concrete ways and means of increasing the interest of the Romanian army soldiers in taking part in such a selection process, which does not always end with participation in multinational operations led by NATO and the EU?

In this context, the research aimed to analyze the internal mechanisms of the human resource generation and regeneration system, with the aim of transforming it into a modern one based on concepts verified in military actions, normative regulations similar to those in other NATO and EU member states. Thus, we considered carrying out a SWOT analysis (Strengths, Weaknesses, Opportunities and Threats), in order to identify those provisions of the existing legislation that should be modified at the level of the military institution, in order to determine their impact on the selection process of soldiers for multinational operations.

In terms of data collection, we used the technique of research and documentary analysis of representative documents, accepted at institutional level, within the NATO member states, the EU or our strategic partner, the United States of America (USA), these being mentioned in the bibliography. The sources analyzed provided us with an overview of the subject addressed and contributed to the effective understanding of the research results. The analysis carried out considered

both the current geopolitical and geostrategic context, but also the existing trends within the NATO and EU member states in terms of attracting human resources and recent developments in this field.

In order to maintain the relevance of the research, in the analysis we considered, in addition to various documents developed during the early period of the Romanian Army's participation in multinational operations, the time interval 2020-2025, which allowed us to obtain a correct assessment of recent trends and developments in the field of human resources.

Starting from the need to streamline the conceptual, normative, organizational and action-oriented process of generating and regenerating structures involved in multinational operations, we have continuously followed those current elements resulting from the participation of Romanian military personnel in foreign missions, so as to ensure not only an element of concreteness throughout the scientific research, but also to generate a new type of approach, which would ensure the adaptation of the system addressed to similar systems in NATO and EU member states. Also, in this regard, we have considered the need to identify those mechanisms and paths of action that would allow the development of a modern process of generating and regenerating military units and subunits participating in multinational operations.

Considering the two research methods, the analysis carried out was organized on two important levels.

a. The first research direction targeted human resources management in order to participate in multinational operations with an emphasis on important aspects such as the regulatory framework aimed at regulating the participation of the Romanian Army in military actions carried out outside the national territory, the organization and conduct of the human resource selection process for this type of military actions, respectively the normative, organizational and procedural streamlining of the entire process of generation and regeneration of the military, through the lens of SWOT analysis..

b. The second research direction aimed to identify the particularities of the process of generation and regeneration of military personnel who take part in multinational missions abroad, with an emphasis on presenting some of the aspects of the organization and conduct of the selection process in order to complete the existing

regulatory framework, respectively identifying those specific measures for preparing the redeployment and reinsertion of personnel participating in multinational operations.

SWOT analysis is usually used to provide an overview of an organization, respectively to collect the information necessary to protect its interests (Ivorschi, 2012). From an institutional perspective, we believe that this type of analysis allows for a concrete radiography of the normative evolution of the process of generation and regeneration of forces and ensures the quantification of the internal and external influencing factors that act on it, in relation to the other processes that take place at the level of the military institution, in order to highlight the strengths and weaknesses of the specific stages of the process addressed in direct relation to the opportunities and threats identified.

In the analysis carried out, we identified a series of strengths of the process of generating and regenerating human resources, from a legislative perspective, through which the selection of human resources intended for participation in multinational operations is ensured, respectively through which the mechanisms necessary for carrying out an organized and planned approach are generated.

Strengths	Weaknesses
● the good physical, psychological and medical condition of the personnel of the Romanian Army and the high level of professional training; ● the efficient process of periodic verification, from a physical, psychological and medical point of view; ● the level of remuneration, corresponding to participation in multinational operations; ● the existence of an appropriate work climate that creates conditions for the military to maintain a high level of training.	● the differentiated initial level of training of soldiers taking part in multinational operations; ● the regulation of the selection method of soldiers participating in operations abroad does not require a clear record of their physical and mental health status, over a determined period; ● the difficulties encountered in planning the resources allocated to the selection process; ● the uncertainties registered among those participating in the selection process.

Opportunities	Threats
● increasing the level of training of participants in multinational operations; ● achieving an appropriate balance between the number of participating soldiers and the budgetary allocation; ● streamlining the selection process determines the formation of a reserve for rapid replacement of soldiers, in a short time; ● ensuring sufficient reserves capable of ensuring the conduct of military actions, under optimal conditions; ● increasing the level of professionalization, by executing additional missions; ● increasing the level of interoperability of structures engaged in theaters of operations.	● the general aging of our country's population and implicitly of candidates for participation in multinational operations creates difficulties in terms of military selection; ● overestimation of self, of some of the military deployed in theaters of operations generates the accumulation of frustrations related to the level of salary, the importance given to their work; ● lack of jobs on the domestic market which implies a faster adhesion of candidates for joining the military institution; ● numerous departures from the army, before the completion of the first contract generates problems for the structures that organize selection processes for multinational operations; ● participation in multinational operations of military personnel can generate a distorted image regarding the missions of the structures intended to participate in such military actions; ● numerous fluctuations regarding the level of salary of military personnel, negatively influence their motivation for joining the military profession.

Considering the strengths and weaknesses, opportunities and risks mentioned in the SWOT matrix, we wish to develop these aspects as follows:

- the personnel serving in the Romanian Army benefit from an appropriate physical, psychological and medical situation, undergoing not only a strict selection process, but also a specific training process that ensures a volume of knowledge corresponding to the functions for which the military personnel are selected;
- once entered in the military institution, army personnel, regardless of the way in which this approach was achieved and the rank held/obtained (both those who entered via the indirect path and even more so those who followed the direct path) are periodically subjected, according to the training and instruction plans (Stoica, Viorel, 2015, pp. 37-38), to thorough periodic checks both physically (biannually), psychologically (annually), and medically (annually), which ensure appropriate conditions for them to fulfill their tasks in their job descriptions, during their participation in multinational operations;
- the level of remuneration, together with other benefits provided to the military, represents a way in which the Romanian Army fulfills its obligations towards them, consequently expecting them to be able to fulfill their assigned missions at any time;
- ensuring an appropriate work climate to achieve a planned and expected combat potential generates high expectations and responsibilities for the military to maintain their level of training, including through individual study, so as to allow the structures they are part of to fulfill their missions received both in peace, crisis and war, as well as in multinational actions aimed at collective security (Palaghia, Mihai, 2004, pp. 1-2).

The identified strengths contribute to obtaining answers to questions such as those that highlight the need to reform the military selection system for multinational operations. Some of these questions directly concern human resources and focus on the skills and performance of the Romanian military personnel, the advantages arising from the quality of its own personnel and the experience accumulated in various positions prior to their participation in military actions outside national

borders. Other questions to which we obtained expected answers, both positive and less positive, considered the experience of the management teams (decision-makers) and the degree of optimization of decision-making processes, the resources allocated to participation in missions, as well as the technology of the equipment used in this type of military actions. Taking these strengths into account, in the decision-making process, these aspects would lead, in our opinion, to enhancing the attractiveness of the military profession and to creating a certain behavior of experimentation among those aspiring to a career in this field. Last but not least, it would ensure changes to the regulatory framework in accordance with the expectations of both management structures and those of participants in this type of operations.

Regarding the weaknesses, the research conducted allowed us to identify some aspects that, although known, are not addressed properly, so that their effects are, if not eliminated, at least minimized. In this regard, we would like to highlight:

- the level of training of soldiers taking part in multinational operations is differentiated, which creates the premises for inappropriate behavior in extreme situations, in which the soldier is asked to act;
- the regulation of the selection method of military personnel participating in operations abroad does not also aim at an appropriate level of training (scales to be met, results for a previous period of time, medical and psychological observations that ensure a clear and appropriate record of their physical and mental health status);
- the resources allocated to the selection process (human, material, financial) often require supplementation, due to the selection being repeated several times for certain positions, which ultimately represents a loss that no one can compensate for;
- the activities specific to the selection tests create a series of uncertainties both among the participants in the selection process and their commanders, since this type of activities is carried out routinely, every year – medical visits, physical and psychological testing, command training, knowledge of foreign languages, driving and psychotechnical testing for staff personnel.

As in the previous case, the research carried out involved obtaining answers that are usually considered when analyzing weaknesses, such as identifying weaknesses in the selection process, what the level of training should be to allow soldiers to participate in multinational operations, or the behavioral deficiencies that we must consider in carrying out this approach.

On the other hand, questions regarding the level of attachment of the soldiers to the structures they are part of, the existence of financial resources throughout the mission period or the appropriate estimation of the costs to be recorded provided as many answers that came to complete the analysis carried out. Last but not least, another set of questions to which we aimed to obtain answers concerned the possibility of outsourcing, through procurement, of some services in the mission area, including personnel, possible unforeseen expenses generated by the extraction/introduction of soldiers from/into the theater of operations or organizational management questions related to the successful or not carrying out of actions in theaters of operations without repeating the mistakes made previously. Taking concrete measures that would contribute to streamlining and making the selection process of military personnel participating in multinational operations more flexible would ensure not only the modification of the regulatory framework, in the sense of eliminating some of the weaknesses, but also the minimization of most of them, with beneficial results for the structures nominated to be deployed in theaters of operations, respectively for the selection process of staff personnel.

From the perspective of the identified opportunities, we consider that they must be exploited to the fullest extent so as to ensure the increase in the degree of interoperability and compatibility of the Romanian force structures with similar ones belonging to other NATO and EU member states. In this regard, we consider the following aspects to be opportunities**:**

- increasing the level of professionalization (training) of all military personnel involved in multinational operations (Alexandrescu, Duţu, 2007, p. 21);
- achieving an appropriate balance in terms of the ratio – number of soldiers and budgetary allocations, given that the decrease in

the number of soldiers (through professionalization) balances the budget allocated to their training;

- by increasing the efficiency of the selection process, the formation of a reserve for rapid replacement of soldiers or subunits in the theater of operations is ensured, in a short time;
- eliminating the dysfunctions created in the selection process, through the aging of the population and ensuring sufficient reserves capable of ensuring the conduct of military actions, under optimal conditions, even in conditions where the initial training of these soldiers is different;
- increasing the level of training of military personnel participating in multinational operations allows them to carry out missions that are not included in their job descriptions;
- increasing the level of interoperability of the structures engaged in theaters of operations ensures the conduct of joint actions with other units and subunits belonging to NATO and EU member states, under appropriate conditions.

The questions aimed at clarifying the identified opportunities and which should be leveraged to the maximum, considered the answers obtained when verifying hypotheses. These included: what changes in the external environment that could be exploited; what types of programs for equipping the armed forces with modern technology and equipment will be implemented in the near future, from the perspective of global technological advancements; what behavioral changes occur among military personnel participating in multinational operations both during selection process and after returning from missions.

Another aspect of the research into available opportunities concerns the military selection system from a strategic and operational point of view, the answers to questions regarding the need for diversification or specialization of activities specific to selection or how we can act in terms of attracting human resources, by creating organizational advantages that ensure participation in these foreign operations, with a multinational nature.

The existence of these opportunities can lead, in our opinion, to an acceleration of the transformation process in the field of human resources aimed at creating a new advantageous regulatory framework

for those participating in the selection for multinational operations. The concrete measures that should be considered by decision-makers in the field addressed could contribute to the creation of a modern system, perfectly aligned with similar systems within the member states of the North Atlantic Treaty Organization and the European Union.

The identified threats can generate operational difficulties among the military and the structures they are part of, which can contribute to the poor performance of the tasks received. From this perspective, we believe that the threats identified during human resources research must be addressed directly in order to eliminate them or reduce their adverse effects as much as possible.

Thus, we have identified some threats, as follows:

- the general aging of our country's population and implicitly of candidates for the profession of arms, creates a new, quite challenging trend as a result of the increase in the number of professional soldiers and the excessive modernization of military technology and equipment, which creates difficulties in terms of the selection of soldiers for participation in multinational operations;
- the existence, even after several years of participation in multinational operations, of a small number of positions within the structures that take part in such military actions generates a series of cumulative tasks, not specified in the job description, which usually denotes an unrealistic overestimation of self of some of the soldiers deployed in the theaters of operations and generates the accumulation of frustrations related to the level of salary (compared to other soldiers), the importance given to their work, etc. (Alexandrescu, Duțu, 2007, p. 23);
- another threat concerns the lack of jobs on the domestic market, which implies a much faster adhesion of those wishing to join the military institution. This fact most often leads to the acceptance of candidates with a low level of training within the military institution, which creates difficulties later in the training process on a technique with a high technological degree;
- the difficulties encountered in the training process, in a system with a different level of organizational culture, generate

untimely departures from the army, unprepared, respectively before the completion of the first contract. In this sense, the disorder created by these departures creates numerous problems for large units, military units and subunits that organize selection processes for multinational operations, respectively for maintaining their level of operability;

- participation in multinational operations of staff and military structures (by rotation), in addition to the numerous benefits, can also generate a distorted image of the tasks and missions of these large units and units, which must first and foremost aim at national and collective defense, alike. This image must be permanently corrected through various corrective measures that target the entire spectrum of socio-behavioral activities, including training, in which the military are involved;
- the numerous fluctuations regarding the level of military salaries, as well as the discussions in the public space regarding the security of their incomes, generate a series of various deficiencies, from the perspective of the selection process of military personnel who wish to participate (voluntarily) in multinational operations, among which the impact on the motivation for joining the military profession would be the most important, from our point of view (Alexandrescu and Duțu, 2007, p. 24).

The identified threats and the answers to the questions that aimed to address this level of the analysis carried out highlighted the need to increase the attention of the management bodies at all levels of the military system, which must find urgent ways and means to resolve them in order to balance the human resources system, which is in obvious difficulty. In this regard, the questions to which we sought to obtain answers concerned the existing legislative framework and the need to make changes that would support the selection process for participation in multinational operations, including through proposals that would consider the social norms and lifestyles of the military, in the new geopolitical and geostrategic context in which we find ourselves.

Changes in the technological field, those specific to goods and services offered to the military must quickly find answers that contribute to increasing their desire to participate in multinational operations. Last

but not least, the difficulties encountered in the field of recruiting labor for the military system must be resolved through well-thought-out measures that provide predictability and security in the evolution of the military within the Ministry of National Defense, regardless of the structures they belong to.

Ways and means of efficiency improvement

The research conducted on the ways and means of streamlining the selection process of military personnel for participation in multinational operations focuses, in our opinion, on the way in which the selection tests are established and then their order. In this regard, there are opinions in the military environment for and against the conduct of these selection tests and the way in which the entire process is organized. Easier said than done, would say some of those who have become outspoken critics, for various reasons, of the selection process. What should be changed in the way the selection tests are organized and ranked, so that, in the end, we can obtain from the first selection period the necessary number of military personnel to fill the structure, as follows: medically healthy and psychologically fit; with an appropriate level of knowledge of the English language; capable of prolonged physical effort and, on top of that, who are also specialists in a position to fulfill their assigned missions?

In our opinion, a deep and complete re-establishment of the entire selection process on modern bases is necessary, which would gather the best practices in the field and the lessons learned from similar experiences of some of the armies of NATO member states, with an additional emphasis on the way in which human resources are attracted in states such as the USA, Great Britain, France, Germany or the Netherlands. Overlaid on the experiences recorded at the level of the Romanian army, we believe that we could, in this way, achieve a specific, efficient and effective process. From this point of view, taking into account the character and specificity of the human resource within the Romanian Army, we believe that an efficient process of selection of military personnel for participation in multinational operations should take into account the clarification of organizational aspects that aim at the way of carrying out the entire process and providing coherent and

natural answers to questions such as those that allowed the analysis performed in the research activity (SWOT analysis). Natural questions to which we often either do not find consistent answers, or we offer explanations that do not have the gift of clarifying us regarding a more efficient approach to the selection process for multinational operations.

Considering the above, we believe that streamlining the selection process for Romanian military personnel participating in multinational operations within the UN, NATO, EU, and OSCE should take into account, in addition to the voluntary expression of acceptance/desire to participate in such military actions, although here too there would be many arguments for and against, the following aspects:

- conducting a single selection stage, in two steps, with the participation in the first step of the military personnel from the structure nominated to take part in the multinational operation, and in the second step of the military personnel from the structure representing the upper echelon of the first unit, to complete the personnel reserve, respectively the deficit by function, when registered (for single functions this process can reach up to the level of force category command and support command);
- considering, for the purpose of recruitment, the physical fitness tests, medical and psychological visits completed by the military, in accordance with the legal provisions in force in the military institution;
- completion of the entire mission-specific training program by all military personnel, base and reserve, including foreign language training hours;
- introducing periodic mid-mission checks to highlight their level of training and to make the military aware of the need to achieve the standards required for participation in the multinational operation;
- the execution of the final verification, without the right to appeal, by the candidates, visibly, in full transparency, which will ensure the retention among those who will participate in the mission of the military who have understood to fulfill the tasks and responsibilities assumed by the contract, in the best conditions. For those who for various reasons could not pass

the final tests, it is the duty of the units to which they belong to be introduced to intensive training/medical monitoring/other type of training programs, which will allow them to reach in a short time the physical and psychological state necessary to fulfill the obligations assumed by the contract. Otherwise, the decision-makers should decide what will be the way forward in this type of situation, including their transfer to some specific functions in the administrative field.

What would be the conditions for such a selection process to be carried out in good conditions, without generating additional expenses and ensuring the participation in the multinational operation of the most deserving, well-prepared military personnel from all points of view? First, increasing the efficiency of the process of attracting human resources (physical, psychological tests, medical visits carried out transparently, without waiving specific standards), secondly, generating a competition between potential candidates for access to the military system, reviewing the processes and training plans to ensure the accumulation of appropriate knowledge, maintaining the physical and mental qualities of the military personnel, once selected, respectively thorough, extensive medical visits, which would lead to the removal of some of the candidates with gender issues from this endeavor.

Furthermore, we believe that a change in the approach to medical visits, in which family doctors would have a correspondent role during the selection (the military personnel being obliged to bring medical observation sheets from them), with the families of the military personnel ensuring the detection of possible mental problems, difficult to detect even in the case of specialized tests, the creation of sports facilities at the level of military units, would be desirable and would not only provide valuable information for the members of the selection teams, but would also contribute to a more efficient use of both the time and resources allocated, at this time, to this process.

Conclusions

At the end of this article, we consider it is necessary to draw attention to some of the situations that have occurred over time, in one form or another, in this type of process carried out at the level of many

of the military units of the Romanian Army. Thus, many of the situations that have arisen over time during the selection process for participation in multinational operations could have been avoided, through the care of the personnel (decision-makers) who manage the admission processes into the ranks of the armed forces, respectively the training processes at the level of military units.

We can look back and think that by taking all the necessary measures (effective command training, physical training to existing standards, effective and carefully monitored medical visits, permanent training and verification regarding the level of knowledge of foreign languages, etc.) the rate of candidates who do not pass one or more of the selection tests for participation in such missions would have decreased considerably. On the other hand, we believe that the measures that have been taken over time to manage this process not only did not accelerate its efficiency but, in many cases, even contributed to its blockage, to a certain degree of habit, like "let it continue as is", on certain limits that it would not have been good to maintain. Of course, it is very easy to observe and offer solutions. From this point of view, we believe that all those involved in this normative, legislative, operational and administrative process have present and future responsibilities.

Important steps towards streamlining the process of attracting human resources, respectively of selection for participation in multinational operations, have been made, especially in the last period of time. One aspect worth highlighting would be the transition of military selection from a centralized system, at the level of zonal selection centers, to a decentralized system, at the military unit level, which would allow attracting a larger number of military personnel and would contribute to reversing the process of entries versus exits from the army, in favor of the first situation. Last but not least, the increase in the attractiveness of the functions in the military system has generated much more important entries in the last period of time. The idea of maintaining the balance between those who want to join the Romanian army, who want to participate in multinational operations and the obligations that they assume through the signed contracts is important.

References:

1. Alexandrescu, Grigore, Petre, Duţu. (2007). *Optimization of the regeneration of the Romanian Army structures engaged in military actions outside the national territory*, Publishing House of the National Defense University "Carol I".

2. Armée Canadienne, http.//www.army.force.gc.ca/lf/Français/5.

3. *Doctrine for multinational joint operations*, Bucharest, 2001.

4. *European Union Concept for Force Generation*, Brussels, November, 2015.

5. *Force generation plotting the way forward for Canada's Army*. https://www.espritdecorps.ca/interview/force-generation-plotting-the-way - forward-for-canadas-army.

6. Grigoraş, Răzvan. (2022). *Prospective Scientific Methods in National Security*. Top Form Publishing House.

7. Ivorschi, Rodica. (2012). "SWOT Analysis – a managerial tool for making activities more efficient." *Romanian Statistical Review*, no. 5, pp. 58-65.

8. Law no. 80/ 1995 on the Status of Military Personnel, published in the *Official Gazette of Romania* no. 155/1995, with subsequent amendments and supplements.

9. Law no. 346/ 2017 on the organization and functioning of the Ministry of National Defense, published in the *Official Gazette of Romania* no. 867, November 2, 2017.

10. Law No. 121/ 2017 on the participation of the armed forces in missions and operations outside the territory of the Romanian state, 17 March, 2017.

11. Lungulescu, Marilen, Alexandru, Adomnicăi. (2014). "Human resources in the Romanian Army, on the path of interoperability with similar structures in the armies of NATO member states", *Romanian Military Thinking Magazine*, no. 2, pp. 31-42.

12. *Manual of personnel support in operations,* Bucharest, 2014.

13. M. 101/2011. Order for the approval of the criteria and methodology regarding the selection of personnel for participation in missions and operations outside the territory of the Romanian state, Bucharest, 2011.

14. M. 59/2015. Order for the approval of the Norms regarding the organization and conduct of the competition/examination for the occupation by the personnel of the Ministry of National Defense of permanent positions in the national representation structures abroad, as well as those in the international structures to which Romania is a party, with subsequent amendments and completions.

15. *NATO's Force Generation and Deployment*. www.gmfus. org ›publications

16. Neag, Mihai. (2004). *Prezent şi perspective privind participarea României la acţiuni NATO*. armyacademy.ro/reviste/1_2004/Prezent%20şi%20perspective.pdf

17. Operation in Iraq. Lessons for the Futur, http://www.globalsecurity.org/military/ lbrary/rapport/2003/iraqops.lessons/ukmod.dec 03chap1.htm.

18. Palaghia, Mihai. (2004). "Principles and content of the force generation and regeneration system." *Strategic Colloquium*, No. 15 (XXVII), pp. 1-4.

19. Pînzariu, Sorin, Bixi-Pompiliu, Mocanu. (2016). *Logistics Guide for Theaters of Operations*. "Carol I" National Defense University Publishing House.

20. Stoica, Viorel. (2015). "The reserve of forces and the mechanism for replenishing losses in military actions." *Bulletin of the National Defense University "Carol I*", no. 34-40.

21. SMAp-S-96, Provision for establishing operational responsibilities regarding the training and management of military structures and personnel participating in missions and operations outside the territory of the Romanian state, Bucharest, 2018;

22. *Troop contributions – NATO*. www.nato.int › topics_50316.

23. *The Power of NATO's military*. https://shape.nato.int/knowing-nato/episodes/the-power-natos-military.

HISTORY AND MEMORY IN INTELLIGENCE

INTELLIGENCE, SECURITY CULTURE AND PUBLIC PERCEPTION

Bogdan GHEORGHIȚĂ*

Abstract:
This article examines the concept of security culture through a multidisciplinary lens, combining theoretical insights with case studies and empirical data. By reviewing recent and influential publications on intelligence services – including works on the Mossad, the CIA, the FBI, and the Soviet KGB/GRU – the study identifies recurring operational patterns, organizational cultures, and public perceptions that shape contemporary security environments. The analysis draws on both primary sources, such as declassified operations, and secondary data from public opinion surveys conducted in Romania, highlighting the evolving relationship between intelligence institutions and democratic societies. Particular attention is given to how literature and media representations influence public understanding of intelligence activities, complementing official communication channels. The article concludes that a robust security culture – built on cognitive, affective, and evaluative dimensions – is essential for strengthening democratic resilience in the face of modern threats such as terrorism and cyber-attacks.

Keywords: *security culture; intelligence; CIA; Mossad; FBI; public perception; national security; Romania.*

Introduction

The world of intelligence services has both fascinated and intrigued people since ancient times. The analyses that have always been essential to political decision-makers in every country have been conducted through a wide variety of methods. Among these, human resources – field agents who collect information and maintain direct contact with the reality of the tactical environment – stand out as the most important. The activity of gathering intelligence regarding the intentions of an "unfriendly" state is not only dangerous, as anyone can imagine, but also difficult to sustain over the long term.

* Lecturer PhD, "Lucian Blaga" University of Sibiu, email: bogdan.gheorghita@ulbsibiu.ro

In recent years, literature addressing the activities, tactics, successes, and failures of intelligence services around the world has been enriched, for the Romanian public, by several works that clarify such matters, presenting the "world" of intelligence services and, in particular, that of secret agents, with all its different accents: double lives, money, planning, unexpected victories, revenge, and intrigue. These documentary-style books can serve as an opportunity for reflection on how information is collected and subsequently used by the consumers of intelligence. Moreover, they help us understand the role of intelligence services in a broader sense, as well as the motivations of those who work undercover in this field.

We refer to them as *documentary books* because, regardless of the form they take – whether monographic or slightly speculative – each documents the activities or events described by relying on a range of verifiable data and facts. In this respect, such publications, intended for the general public, contribute to explaining and understanding various operational methods, reveal activities, or present facts about which little is otherwise known. Thus, works that document the activities of intelligence services play a particularly important role in shaping security culture, by helping to clarify the role and place of intelligence services within a democratic society.

The central research question guiding this study is: To what extent do social representations and documentary literature influence the consolidation of a democratic security culture? First, we will briefly explore the concept of *security culture*. Then, from a descriptive perspective, we will highlight several such editorial works in an attempt to outline some reference points concerning the cognitive dimension of security culture. In a certain sense, the public becomes acquainted with the activity of intelligence services through such publications. Starting from the general knowledge about the intelligence system, taking into account its structural components and the relationships between them, we can later observe the attitudes and behaviours built upon this foundation. The image of intelligence services is continuously constructed, and an important dimension of this image can be verified through opinion polls. In this regard, we will use several national and local surveys to better understand what Romanian citizens know about this

"world" and to identify the main reference points in their perceptions regarding intelligence services and their activities.

Security Culture: An Overview

Security culture is currently studied more intensively by specialists, as recent events and the present context have provided a strong impetus in this direction. However, much like in the case of political culture, an operational approach is required to avoid the trap of assuming that it merely concerns the existence of an informational stock on the subject.

In their book *The Civic Culture: Political Attitudes and Democracy in Five Nations*, Gabriel Almond and Sidney Verba (1996) comparatively examine the characteristics of political culture, as well as the social structures and processes involved. The study, conducted in the second half of the last century (1958-1960), is fundamental for understanding the political behaviour of individuals as a result of the internalization of values, beliefs, or knowledge that shape political culture. In other words, political culture provides support – a motivational foundation – for various political attitudes that later translate into behaviour. Without delving into the more complex findings of the two authors, we shall highlight how they analysed the concept of political culture, operationalizing it in order to make it measurable.

Understanding political culture as "a set of orientations toward a special set of social objects and processes" (Almond and Verba, 1996, p. 43), the authors identify three main components of the internalization of these orientations at the individual level:

1. Cognitive orientation – knowledge and beliefs regarding the political system, its roles, role holders, inputs, and outputs;

2. Affective orientation – feelings toward the political system;

3. Evaluative orientation – judgments and opinions regarding political objects (Almond and Verba, 1996, p. 45).

In other words, the political culture of a group of individuals, regardless of size, consists of a cognitive dimension (what they know about the political system they live in), an affective dimension (how they feel toward their political system, relative to its roles), and an evaluative dimension (how they assess the political system, based on information and feelings). This makes the study conducted by Almond and Verba

essential. Following this model, we can operationalize the concept of *security culture*, analyse it systematically, and measure certain components of it at individual or group levels. Otherwise, we risk discussing "culture" (of any type) too generically, emphasizing the quantitative aspect of the information possessed – which, most of the time, is not even comparable.

Recently, studies have explored the balance between democracy and surveillance, or information gathering in today's society (De Graaff, 2016), while other authors have discussed the importance of social perceptions within the concept of security culture (Chiru, 2016) or the awareness of risks at the societal level (Nicula and Teodor, 2016). In Romania, the security culture – in which citizens understand the role of intelligence services and support their activity – still bears the burden of the past. Fear of intelligence services took shape during the communist period, when contact with intelligence officers was not desired. The ongoing dialogue between post-communist intelligence services and society as a whole, within the context of democratization, represents an essential element in building a genuine security culture (Chiru, 2014). Increasingly, studies have addressed the importance and characteristics of security culture (Matei and Halladay, 2019) within new geopolitical contexts and in light of growing multidimensional threats.

Security culture clearly constitutes an essential framework for a safer society. If we apply Almond and Verba's formula, we can discuss three dimensions of internalized orientations at the individual level:

a) **Cognitive orientation** – what we know about institutions and their roles;
b) **Affective orientation** – feelings toward security institutions;
c) **Evaluative orientation** – judgments and opinions.

Surveys and interviews could help clarify these dimensions. Certain publications make known to the Romanian public the activities of various intelligence services. How these services operate, the ways they accomplish their missions, their organizational structures, and their successes or failures can all contribute to understanding their roles within the democratic institutional framework. Such a perspective can at least help structuring the cognitive dimension. This definition integrates the elements of security culture as "the totality of notions, ideas, and

information possessed, at a given time, by the citizens of a state, concerning the values, interests, and security needs that form and develop attitudes, motivations, and behaviours" (Nițu, 2012).

When discussing the field of security as represented in various publications, the general public comes into contact with it through engaging works of interest. Some of these belong to former intelligence officers who "reveal" techniques and methods of action that may be useful in everyday life. Such works appeal to readers who imagine that professionals in this field possess "secrets" that make them invulnerable. Among them we can mention *Think like a Spy* (Fisher, 2025) and *Becoming Bulletproof: Strategies for Your Own Security* (Poumpouras, 2022).

Other authors present the domain of security in a structured manner, explaining in detail the intelligence cycle, contemporary challenges, and the importance of the human resource (HUMINT) in intelligence work – for instance, John Hughes-Wilson's *The Secret World: A History of Intelligence* (2017). Some works are written by former intelligence service directors, whose insights can offer readers either a comprehensive overview, details from inside the profession, or geopolitical trends at regional and global levels – such as *The Mossad Director: Doctrine and Missions of Israel's External Intelligence Service* (Shavit, 2021).

Chris Whipple, in his book *The Spymasters: How the CIA Directors Shape History and the Future* (2024), analyses the mandates of U.S. intelligence directors, explaining their relationships with the president and the ways in which intelligence is used by political decision-makers.

There are also works written by historians, sometimes spanning hundreds of pages, which trace the evolution of intelligence services or the development of the "world" of espionage from ancient times to the present. Notably, Christopher Andrew's *The Secret World: A History of Intelligence* (2022) is an exceptionally well-documented study that relies on reliable sources and official documents, tracing the evolution of intelligence services from the era of Sun Tzu to September 11, 2001 – a turning point in global intelligence approaches. Such works, like that of the British historian, seem particularly relevant for specialists and readers passionate about the field.

Next, we will analyse several publications that can offer reference points regarding how representations of this domain are constructed. Attitudes and behaviours are based on what we know – or believe we know – about reality. In the following section, we will examine several recent works to clarify certain reference points and dimensions of our representations concerning the "world" of intelligence services and their activities and roles.

From a methodological standpoint, this study adopts a qualitative and exploratory approach, combining the analytical review of recent documentary works on intelligence and national security with the interpretation of secondary data derived from public opinion surveys. The objective is to identify and discuss the cognitive, affective, and evaluative dimensions of security culture as they emerge from public representations and cultural narratives.

Eli Cohen: The Lone Wolf of Damascus

Under the signature of Samuel Segev, a figure closely connected to Israel's intelligence community, Corint Publishing House released the book *Alone in Damascus* (2019). The work recounts the story of Eli Cohen, arguably the most famous secret agent in the history of the State of Israel.

Eli Cohen carried out espionage activities in the Syrian capital from early 1962 until January 1965, when he was captured. Known as "Fighter 88" within the operational structure to which he belonged in Israel, or as "Menashe" in intelligence reports – used as an additional layer of protection – Eli Cohen provided vast amounts of crucial information to political decision-makers. Under the assumed identity of Kamal Amin Thaabet, an Arab businessman recently returned from Argentina, Cohen swiftly established close connections with several high-ranking Syrian officials and military officers, who provided him with essential intelligence regarding Syria's intentions and actions toward Israel.

Charismatic, "Thaabet" skilfully exploited both the vulnerabilities of the Syrian political system and the internal power struggles in Damascus, as well as the personal weaknesses of those with whom he interacted. By organizing discreet social gatherings for political and

military elites, raising funds for political causes, and offering loans to his Syrian acquaintances without expecting repayment, "Kamal" became so deeply embedded in Syrian society that he practically identified with it. The path to this point, however, was far from easy. To construct such a credible identity, Eli Cohen underwent a complex and demanding training process: he enhanced his memory skills, learned counter-surveillance techniques, and mastered the art of disguise (Segev, 2019, pp. 108-123).

He later relocated to Buenos Aires, where he established connections with members of the city's Arab community and obtained letters of recommendation for his later use in Damascus – thus lending authenticity to his cover story. Once in Damascus, he managed to befriend influential figures across all power circles, gathering information from both civilian and military sources. His contacts came from the highest decision-making levels. Cohen's hundreds of Morse code transmissions, relayed to Israeli operatives in Europe, proved strategically invaluable to Israel for organizing combat capabilities and military operations along the Syrian border (Segev, 2019, pp. 209 and 243).

Eli Cohen identified and communicated to Israel the strategic positions of the Syrian army on the Golan Heights – a fact that proved decisive in Israel's capture of the plateau during the June 1967 war (Segev, 2019, p. 11). Though intelligence work comes at a cost, its benefits are undeniable in situations such as these.

Segev's book, structured in eleven chapters, traces the major moments of Cohen's career – from his initial attempts to join Israeli intelligence services, to his recruitment, specialized training, creation of his new identity, and infiltration into Syria. Beginning with Cohen's capture in Damascus in January 1965 – a well-known event in Israel's collective memory (Segev, 2019, p. 51) – the author builds the narrative in a fast-paced, documentary style reminiscent of a spy novel. Evidence, official documents, intelligence sources, and excerpts from Cohen's interrogation are presented throughout the book. To some extent, the structure mirrors that of a film, featuring suspenseful moments and storylines that unfold gradually across chapters.

Beyond the operational success achieved by the Israeli agent, the book also gives voice to his frustrations, struggles, and the immense

burden of his mission. Alone in the Syrian capital, without a support network, Cohen appears vulnerable and constantly exposed to danger – far more than agents operating within coordinated teams. Yet this very solitude may have been his greatest advantage. Acting as a "lone wolf" might have provided him with perfect cover: he did not need to meet other agents, use safe houses, or engage in routines that could raise suspicion. When the Syrians finally captured him, they sent a telegram to Israel implying that they believed Eli Cohen to be the head of an extensive spy network operating inside Syria (Segev, 2019, p. 59).

His continued success was likely aided by his constant changes in message encryption techniques. After each trip abroad, he received a new code and often a new transmitter, which he used upon his return to send the most critical reports to Israel.

Yet, as Segev clearly points out, toward the end of his mission Eli Cohen became overconfident in his own abilities and tactics. Believing himself nearly untouchable, he began to disregard the strict operational limits of his transmissions (a maximum of nine minutes) and reduced the number of messages he sent to Israel (Segev, 2019, p. 48). This ultimately led to his capture by Syrian forces, aided by Soviet-supplied radio-location technology (the Syrians had been unable to decrypt his messages). Cohen was located through the Morse signal emitted by his transmitter.

After his capture, Israel made every possible effort to secure first his release, then his life, and finally the repatriation of his remains. However, none of these appeals succeeded – the Syrians, deeply humiliated by the exposure of their secrets, refused all interventions: not the French lawyer's pleas, not those of Eli's wife Nadia, nor the offers of money, Vatican appeals, or international diplomatic pressure (Segev, 2019, p. 347). On May 18, 1965, at 3:30 a.m., after reciting his final prayer and sending a last letter to his family in Bat Yam, Eli Cohen was executed by hanging in Marjeh Square, Damascus (Segev, 2019, p. 11).

Cohen's mission in Damascus highlights an essential truth for all intelligence services worldwide: the irreplaceable value of the agent on the ground – whose assessments cannot be substituted by any other source. Military personnel often remark that a disputed territory is truly controlled only when an infantryman "sets foot" on it. Similarly, in the world of intelligence, without field agents physically present in the area

of interest, information collected through other channels lacks the same analytical and operational value. Following Cohen's execution, Meir Amit, then head of Mossad, declared in a speech at the Israeli Embassy in Paris:

> "We trained him for two years, and he succeeded in his mission in a way almost unparalleled by anyone else. He established deep contacts with people at the highest levels of the Syrian regime, effectively becoming part of it. Thanks to him, we had a perfect picture of the events unfolding in Damascus. He provided not only data we might have obtained from other sources, but above all, the atmosphere on the ground – a type of information for which there is no substitute." (Segev, 2019, p. 343).

Through the intelligence he transmitted to Mossad, Eli Cohen enabled an accurate understanding of Syria's plans regarding Israel, as well as a precise assessment of the regional situation, leading to appropriate strategic responses. Years later, another Mossad agent, known by the codename "The Angel," Ashraf Marwan – this time an Egyptian official – would provide similarly invaluable information to Israel, used during the Yom Kippur War.

Segev concludes his book with a striking passage:

> "Whatever might have happened, the fact remains that Eli Cohen was the only Israeli spy captured and executed as an Israeli, becoming a symbol for all those who operated in enemy states and were caught, tried, and executed as Arabs." (Segev, 2019, p. 350).

Cohen's mission exemplifies how individual heroism and human intelligence operations can shape collective perceptions of secrecy, loyalty, and national sacrifice. In this way we can understand how public representations of intelligence agents contribute to constructing an idealized image of the intelligence community.

Adolf Tolkachev, the Americans' "Eye" Beyond the Iron Curtain

Especially in the early phase of the Cold War, the Central Intelligence Agency (CIA) struggled to provide U.S. political decision-makers with intelligence on the Soviet Union. The Iron Curtain dividing

Europe was impenetrable to American agents, despite the agency's vast financial resources and in spite of various attempted missions – some verging on suicidal, such as parachuting American operatives into Soviet territory. The KGB (*Komitet Gosudarstvennoi Bezopasnosti*), the Soviet secret police, consistently thwarted any capitalist attempt to "look" beyond the Iron Curtain: it was well prepared and experienced and, above all, suppressed espionage efforts with extreme harshness (Hoffman, 2018).

The Billion Dollar Spy: A True Story of Cold War Espionage and Betrayal, David E. Hoffman's 2018 work, tells the story of Adolf Tolkachev – the Americans' unexpectedly "opened" eye behind the Iron Curtain. Across the book's twenty-one chapters, Hoffman traces both the stages through which the CIA's Moscow station passed in its quest for relevant intelligence on Soviet policy and the winding path that brought the Americans their "billion-dollar" spy, who supplied secrets about Soviet radar and research plans for weapons systems. As in Eli Cohen's case, Hoffman's book reiterates a basic necessity for any intelligence service: accurate, on-the-ground information from engaged individuals who can assess trends and provide explanations – things U.S. spy satellites could not deliver during the Cold War.

The volume is compelling also because it presents various espionage methods and techniques used by CIA officers in Eastern Europe and, more importantly, explains how these methods were invented and then became everyday tradecraft. "Espionage is the art of illusion" (p. 15), Hoffman reminds us, and his book offers an X-ray of intelligence activities conducted in the field. While the narrative focuses on the CIA and Cold War espionage, this type of operation is employed by intelligence services worldwide. The book draws on 944 pages of declassified operational files, most importantly the cables exchanged between CIA headquarters and the Moscow station from 1977 to 1985.

Hoffman discusses contact techniques developed within the CIA by officers who entered service in the 1950s-1960s, such as Burton Gerber and Haviland Smith (Hoffman, 2018). The latter, despite initial opposition from agency leadership, developed the *brush-pass* executed during a "time gap" created to shake surveillance. We also learn about the equipment Tolkachev used: first the miniature Molly spy

camera (whose image quality was insufficient for photographing secret documents), then the Tropel (a camera concealed in a key fob), and finally a Pentax ME 35mm single-lens reflex camera (Hoffman, 2018, pp. 153-158). All this illustrates the long road the American service travelled to obtain relevant intelligence.

Operating in Moscow entailed sustained exposure to one of the most hostile counterintelligence environments in the world[1]. As the author notes:

> "Counterintelligence plays a vital role in the effort by spy agencies to prevent penetration by the same methods of espionage they use against other agencies. During the Cold War, this required a combination of outward vigilance – that is, tracking every move of the KGB and deceiving it whenever possible – and inward scepticism – that is, ensuring that the CIA itself was not the victim of a deception or double agents. Ideally, counterintelligence would be coordinated with intelligence collection, but there has always been a natural tension between the two." (Hoffman, 2018, p. 38).

Beyond the gripping details and tension, *The Billion Dollar Spy* also impresses by portraying the qualities required for this work and the dangers faced by those involved. "Everything we do is dangerous," Tolkachev told his case officer in 1984; the drama of his story intensifies in the book, culminating in his capture by the KGB (Hoffman, 2018, p. 395). In the intelligence world, any misstep means not only failure but also severe repercussions for operations and personnel. Hoffman's account bears this out: Tolkachev was caught after the Soviets received information from their mole inside the CIA, Edward Lee Howard – the only CIA officer to defect from the United States and receive political asylum in the Soviet Union, in 1986.

---

[1] For those interested in the highly disciplined operational methods of the Soviet Union's security services, Victor Suvorov's *The Principles of Espionage* (2016) offers a compelling resource. The volume details the tensions between the KGB and the GRU – the military's intelligence directorate – alongside in-depth accounts of officer training, operational coordination, and the methods employed to ensure maximal efficiency in intelligence work across Western Europe.

Kathy Krantz Fieramosca's portrait of Tolkachev, displayed at CIA headquarters (Hoffman, 2018, p. 422), aptly captures the strain under which the Soviet engineer worked for American interests, photographing thousands of pages of classified documents. For a long time, he was the best source the CIA had in Moscow – a "billion-dollar" spy in the most literal sense – whose reporting kept the Americans abreast of the Soviets' most important military research and, crucially, allowed them to prepare accordingly.

A full material assessment of the intelligence Tolkachev provided was never thoroughly conducted by the Americans, but some preliminary estimates concluded that the value amounted to many billions of dollars (Hoffman, 2018). Numerous U.S. military procurement programs were updated as a result – beyond the raw insight into Soviet intentions. And the price paid to Tolkachev for all this was negligible compared to the intelligence delivered.

The story of Adolf Tolkachev illustrates the ethical and psychological tensions inherent in intelligence work. His actions highlight the paradox of loyalty and betrayal, raising questions about moral justification and personal conviction within espionage. The public can understanding the intelligence as both a field of high moral stakes and profound human vulnerability, and this tension enriches the cognitive and affective dimensions of security culture.

Mossad: the Hidden Force of Israel

The way an intelligence service structures itself in its early stages is a subject less frequently documented. Intelligence organizations have existed – under various forms adapted to their times – since antiquity. Consequently, it is difficult to fully grasp how their formative evolutions have left a mark on the institutions we know today.

In the case of the State of Israel, the book *Mossad: The Bloody History of Israeli Espionage*, published by Litera in 2019 and written by Michael Bar-Zohar and Nissim Mishal, offers readers the opportunity to analyse a series of declassified operations of Israel's secret service, from its inception – events that are, historically speaking, not far removed from our time. The authors' main goal is to present the declassified missions of Israeli intelligence and, more importantly, to illustrate the markedly different nature of the operations carried out by Mossad

officers. These agents act in highly hostile environments, most often without any logistical support on the ground from their headquarters. When captured, Israeli agents rarely benefit from the customary prisoner-exchange practices typical of the intelligence world – such as those conducted during the Cold War between the Americans and the Soviets[2].

In *The Bloody History of Israeli Espionage*, the authors undertake a difficult task: to shed light on "the most important missions and the bravest officers of Mossad, as well as the mistakes and failures that, more than once, stained the agency's image and shook it to its core" (Bar-Zohar and Mishal, 2019, p. 11). The book presents numerous Mossad missions with factual accuracy, also exposing the darker side of certain operations – the assassinations carried out by or on the orders of the Mossad. Among the names mentioned are Rezaei-Nejad, the physicist involved in Iran's nuclear program, assassinated in 2011; Ali Hassan Salameh (the "Red Prince"), mastermind of the terrorist attack at the 1972 Munich Olympics; and Mahmoud Abdel Rauf al-Mabhouh, a Hamas leader killed in a famous operation in Dubai – all vividly described in the pages of the book (Bar-Zohar and Mishal, 2019).

A key chapter in the volume offers a detailed account of the kidnapping of Adolf Eichmann from Argentina and his transfer to Israel for trial (Bar-Zohar and Mishal, 2019). This Mossad operation was one of the most famous of its time and contributed to numerous legends about the agency's methods of action. To understand the importance of Mossad's involvement, it is essential to note that Eichmann's trial in Jerusalem represented a turning point for the Israeli state – perhaps the most significant political event after its founding.

For readers of Bar-Zohar and Mishal's work, the book offers an opportunity for reflection. The region in which the Israeli secret service operates is an extremely complex one, and Mossad's methods are equally diverse. For this reason, its legendary operational successes are often balanced by notable failures.

---

[2] For an in-depth examination of such practices, Giles Whittell's *Bridge of Spies* – first published in 2011 and reissued in 2020—offers valuable insights. The book explores the exchange of prisoners during the Cold War in Berlin, shedding light on one of the most emblematic episodes of espionage diplomacy of the era.

Another work by the same authors, *The Amazons of the Mossad* (2024), discusses the role of *katsa* women – field officers. In the early days of Israeli intelligence, women played mainly supporting roles, accompanying male agents to provide them with better cover. Over time, however, women were accepted as fully-fledged officers, indicating that the struggle for gender equality has also yielded results within the intelligence community.

The Mossad case underscores the complexity of intelligence work within a hostile geopolitical environment, revealing both the operational brilliance and the ethical dilemmas associated with covert action. The Mossad actions lead to a dual narrative – one of national pride and one of moral ambiguity. These representations contribute to shaping the affective component of security culture. For a security service, operational success coexists with questions about legality, transparency, and democratic oversight.

"A Disgusting but Vital Necessity" to Understand and Influence Events Abroad

If the beginnings of the Federal Bureau of Investigation (FBI) in the United States are inextricably linked to the name of J. Edgar Hoover, the history of the Central Intelligence Agency (CIA) – another key and widely recognized component of the U.S. security architecture – lacks such a singular founding figure. Both institutions, with their successes and failures, are thoroughly analysed in Tim Weiner's works. His two major books, *CIA: A Secret History* and *FBI: A Secret History*, were both translated into Romanian and published by Litera Publishing House in 2019.

While the CIA is regarded as the quintessential U.S. intelligence agency, the FBI is often perceived, in the public imagination, as a law enforcement institution. However, the Bureau's counterterrorism efforts and counterintelligence activities mean that many of its operations are, in practice, comparable to those of an intelligence service. Indeed, since its inception, the FBI has had such prerogatives – Hoover's obsession with Soviet influence in the United States being a foundational element of the Bureau's functioning. As integral components of the U.S. security system, the two agencies have collaborated on various levels and

operations. Yet, as with other intelligence organizations worldwide, this collaboration has also been marked by a degree of rivalry.

Both books are extensive and based on a rigorous analysis of official documents concerning the activities of these two institutions, providing a detailed x-ray of their organizational histories. While Hoover's "shadow" continues to loom over the FBI's past, many of the practices he instituted became the foundation of numerous contemporary operational procedures. The strict recruitment standards he imposed, the image he crafted for the Bureau within American society, and the internal discipline he enforced were, without doubt, key elements of its success. Hoover's personal discretion – contrasted with his relentless desire to know everything about everyone else – made him a figure around whom countless rumours were constructed.

What makes Weiner's book on the FBI particularly fascinating is the meticulous way it traces the Bureau's early operations, during a time when many of its activities easily escaped legal oversight (Weiner, 2019). This was largely due to Hoover himself, who built an empire of information encompassing virtually everything that happened within the United States.

President Eisenhower's statement that espionage is a "disgusting but vital necessity" (Weiner, 2019a) resonates strongly throughout Weiner's other book. The CIA was built slowly, over many years, and its beginnings are described as "the failure of the most powerful nation in Western civilization's history to build a first-rate espionage service" (Weiner, 2019a, p. 9). Tracing the agency's evolution to the present day – its involvement in various coups d'état, its role during the Cold War, and the inevitable successes and failures of such a history – Weiner highlights the critical moments when the CIA either receded into the shadows of the White House or stood at the forefront of U.S. policymaking. There were times when presidents side-lined the agency and others when they relied exclusively on its assessments in decision-making, thereby reinforcing its position within Washington's power structure (Weiner, 2019a).

Weiner concludes his analysis by questioning how the agency will adapt to the world of the future. The revival of the CIA – criticized for its role in the flawed analysis of Iraq's alleged weapons of mass destruction – will depend, in his view, on a new generation of agents, visionary leadership, and the substantial resources that the American government appears more willing than ever to allocate to the agency in its fight

against terrorism and hostile states[3]. At least, this is Tim Weiner's own conclusion, with which the book ends.

How Romanians Perceive Intelligence Services

Studies and analyses addressing the public's social representations of intelligence and national security remain relatively scarce. In the early years of Romanian democracy, a 2002 opinion poll conducted by IRSOP (the Romanian Institute for the Study of Public Opinion) examined the public awareness of Romanian intelligence services, the visibility of their directors, and citizens' overall perceptions of these institutions.

When asked how well-prepared Romanian intelligence services were to ensure national security, respondents were divided almost evenly: 48% believed the services were well prepared, while 42% considered them insufficiently prepared, with the remainder being unsure or unwilling to answer (IRSOP, 2002).

As essential components of a democratic state, intelligence services faced a difficult path in post-communist Romania. Burdened by their former image as instruments of repression under the communist regime, these institutions had to convince citizens that they had become pillars of the new democracy. The transition was not easy. A similarly dated but relevant study, conducted in 2004 at the level of Sibiu municipality, revealed that 27.9% of respondents believed intelligence services had not yet transformed into democratic institutions comparable to Western models, while 37.8% believed they had undergone such transformation (the remainder being those without an opinion) (Department of Political Science/ULBS, 2004).

Likewise, 14 years after 1989, 33.3% of respondents in Sibiu believed that some people were still being monitored by special services, while only 27.6% believed such practices no longer occurred (Department of Political Science/ULBS, 2004). Again, the difference up to 100% consisted of respondents uncertain or unwilling to answer.

---

[3] For those seeking further explanations regarding the CIA's failures, James Olson's To Catch a Spy (2020) offers twelve detailed case studies and situates the reader within the contemporary world of espionage. The book elucidates the distinct approaches employed by various global actors, including the United States, China, Russia, and Cuba, providing comparative insights into their operational styles and strategic objectives.

Presenting such survey data today serves more as an "archaeological" exercise – tracing the layers of social representation regarding intelligence services – than as a current assessment. Nonetheless, these findings can help us understand the gradual evolution of public perceptions of intelligence and the foundations of today's security culture.

In March 2014, IRES (the Romanian Institute for Evaluation and Strategy) published a study addressing public perceptions of the Romanian Intelligence Service (IRES, 2014). According to this research, 77% of respondents who had heard of the institution believed that the Romanian Intelligence Service plays a "very important" role. The same percentage (77%) agreed that the agency had undergone reform since 1989.

Although these results cannot be directly compared – given differences in sampling, scope, and questionnaire design – they nonetheless reveal a significant shift from the 2004 Sibiu data, where only about 38% of respondents considered intelligence services to be reformed.

In the absence of longitudinal studies, we can rely only on snapshot data that capture a moment in time without explaining its broader evolution. Still, the public image of intelligence services is crucial because of their role in a democracy. Decision-makers require accurate intelligence reports to make informed choices, while citizens expect a degree of transparency and communication from such institutions – especially today, in a world facing new and complex challenges such as terrorism and cyber-attacks.

Conclusions

Security culture is of paramount importance in today's context. It is grounded in the knowledge we possess about the intelligence system, in the way we relate to it, and in the evaluations, we make regarding its effectiveness. In their activities, intelligence services must operate discreetly. However, in a world where terrorism is no longer a local or regional phenomenon and where cyber threats affect everyone, intelligence agencies must also demonstrate a degree of transparency. Naturally, within a democratic society, such institutions must remain properly supervised and accountable.

In this article, we aimed to review several recent publications – released by relatively well-known publishing houses with solid

distribution networks – in order to clarify analytical frameworks relevant to the concept of security culture. Examining these works helps identify the "lenses" through which citizens perceive the activity of intelligence services. What reaches the general public through this type of literature represents, to a certain extent, what the public knows – or believes it knows – about the field. This type of information and knowledge complements the official communication produced by intelligence services.

Furthermore, by using several secondary data sources – namely, the results of studies concerning the public image of intelligence services in Romania – we have attempted to observe how citizens evaluate these institutions. We believe that understanding these dimensions can offer valuable insights into the state of security culture in contemporary Romania. For greater analytical clarity, a systematic, longitudinal study of the public image of intelligence services – and, more specifically, of Romanians' social representations of them – would be necessary. Such data would help us understand how perceptions of the intelligence system evolve over time and reveal potential vulnerabilities within Romania's security culture.

A security culture that supports democracy could be conceptualized along three main dimensions: cognitive, affective, and evaluative. A systematic study of security culture would enable a deeper understanding of the vulnerabilities and threats we face in the current geopolitical environment.

Two pillars seem to strengthening Romania's security culture: sustained investment in civic education and strategic communication by intelligence institutions. Collaborative programs between universities, think tanks, and intelligence agencies could enhance citizens' understanding of security challenges. By fostering dialogue between the intelligence community and society, Romania can develop a security culture that supports national resilience.

The main limitation of this study lies in the fact that it is based on secondary data and documentary sources. Future research should adopt a longitudinal design and include empirical data collection through surveys or focus groups. In this way we can provide a more comprehensive understanding of how Romanians conceptualize security culture in a rapidly evolving geopolitical environment.

References:

1. Almond, G., and Verba, A. (1996). *The Civic Culture: Political Attitudes and Democracy in Five Nations.* Bucharest: Du Style Publishing House.

2. Andrew, C. (2022). *The Secret World: A History of Intelligence Services.* Bucharest: Trai Publishing.

3. Bar-Zohar, M., and Mishal, N. (2019). *Mossad: The Bloody History of Israeli Espionage.* Bucharest: Litera Publishing House.

4. Bar-Zohar, M., and Mishal, N. (2024). *The Amazons of Mossad.* Bucharest: Litera Publishing House.

5. Chiru, I. (2014). Building an Intelligence Culture from Within: The SRI and Romanian Society. *International Journal of Intelligence and CounterIntelligence, 27*(3), 569–589.

6. Chiru, I. (2016). Social Perception of National Security Risks: A (Missing) Ingredient of Security Culture. *Romanian Review of Intelligence Studies,* no. 16.

7. De Graaff, B. (2016). The Place of Intelligence Organizations in Political Theory. *Romanian Review of Intelligence Studies,* no. 16.

8. Fisher, J. (2025). *Think Like a Spy.* Bucharest: Bookzone Publishing.

9. Hughes-Wilson, J. (2017). *The Secret Services.* Bucharest: Meteor Publishing.

10. IRES. (2014). *Public Perception Elements of the Romanian Intelligence Service.* https://ires.ro/uploads/articole/ires_brand-si-prestigiu-institutional_sri_site.pdf

11. Matei, F.-C., and Halladay, C. (2019). *The Conduct of Intelligence in Democracies: Processes, Practices, Cultures.* Boulder, CO: Lynne Rienner Publishers.

12. Nicula, V., and Teodor, M. (2016). "Risk Perception and Effective Communication Strategies: Interdisciplinary Approaches and Lessons Learned." *Romanian Review of Intelligence Studies,* no. 16.

13. Nițu, I. (2012). *Intelligence Analysis.* Bucharest: Rao Publishing.

14. Olson, J. (2020). *How to Catch a Spy.* Bucharest: Meteor Press.

15. Poumpouras, E. (2022). *Becoming Bulletproof: Strategies for Personal Security.* Bucharest: Meteor Press.

16. Segev, S. (2019). *Alone in Damascus: The Life and Death of Israeli Spy Eli Cohen.* Bucharest: Corint Publishing.

17. Shavit, S. (2021). *The Head of Mossad: The Doctrine and Missions of the Israeli Foreign Intelligence Service.* Bucharest: Litera Publishing.

18. Suvorov, V. (2016). *The Principles of Espionage.* Iași: Polirom Publishing.

19. Weiner, T. (2019). *FBI: A Secret History.* Bucharest: Litera Publishing.
20. Weiner, T. (2019a). *CIA: A Secret History.* Bucharest: Litera Publishing.
21. Whipple, C. (2024). *The Spymasters: How the Directors of the CIA Shape History and the Future.* Bucharest: Litera Publishing.
22. Whittell, G. (2011; 2020). *Bridge of Spies: A True Story of the Cold War.* Bucharest: Litera Publishing.
23. Department of Political Science/"Lucian Blaga" University of Sibiu. (2004). *Public Opinion Barometer – Presentation Report.*

A HUNDRED-YEAR-OLD STORY: THE INFLUENCES OF NEO-EURASIANISM ON RUSSIAN *STRATEGIC COMMUNICATION*

Carla IORDACHE*
Simona ȘERBAN*

Abstract:

As an ideological current, Eurasianism emerged in the early 1920s among young Russian emigrants. It is based on the idea that the Russian people is neither European, nor Asiatic, but bears the influence of both spaces, which gives it unique characteristics. After falling in a cone of shadow during the Communist regime, the Eurasian ideas, reinterpreted under the form of Neo-Eurasianism, have regained popularity during president Vladimir Putin's time in office, generating the neo-Eurasian current, with Aleksandr Dugin as its main promoter. As a result, these concepts have strongly influenced the strategic communication of the Russian Federation, especially after the beginning of the full-scale invasion of Ukraine.

This paper is going to outline the main ideas of both the classical and modern interpretations of Eurasianism, highlighting the resemblances and the differences between the two, and also to identify the influences of Neo-Eurasianist ideas over the Russian strategic communication.

The case study aims to interpret the Russian invasion of Ukraine through the lens of Eurasian ideology, thus providing a new point of view on the actions of the Russian Government and especially of president Vladimir Putin. Moreover, some pieces of information that are part of the propaganda campaigns concerning the invasion will be analysed, in order to highlight the Eurasian influence.

Keywords*: propaganda, Eurasianism, Neo-Eurasianism, Ukraine, Russia.*

---

* Student "Mihai Viteazul" National Intelligence Academy.

* Student "Mihai Viteazul" National Intelligence Academy. Disclaimer: the material is a reflection of the authors' opinions and beliefs, and does not represent the opinions, policies or the views of the Romanian Intelligence Service or the National Intelligence Academy "Mihai Viteazul".

The emergence and development of Eurasianism and Neo-Eurasianism

Eurasianism, as a school of thought, appeared shortly after the First World War and the Bolshevik Revolution, among the young Russian emigrants in Sofia and Prague. The first people to adhere to the Eurasian theory, known as the "classical" Eurasianists were Nikolai Sergeevich Trubetskoi[1], Petr Savitskii[2], Georgii Florovskii[3], and George Vladimirovich Vernadsky[4] (Meyer, 2009). Their writings are centred on the idea that the Russian territory is neither European, nor Asian, but something altogether different. This unique character is the result of special geographical and historical conditions that have led to a seamless blend of three major pillars. The Slavic ethnic substrate is seen as the first of these, which has been developed through the integration of Byzantine traditions and culture, seen as the second pillar. Throughout the history of the Tsarist Empire, this influence has been materialized through the Russian Orthodox Church, an institution that maintains its influence to this day. The third element that defines this unique geographical and cultural area is the existence of state-building elements of Asiatic inspiration (Balatska, 2023). Some authors, such as Nikolai Trubetzkoi, consider this last element to be much more important than the others, The Tsarist Empire and later the USSR being nothing but heirs of the empire built by Genghis Khan (Balatska, 2023). Due to these special characteristics, the Eurasian theory implies that the Russian state, no matter its name, has a unique place in history – that of "re-establishing the rightful, traditional values, in a world that goes through a continuous process of degradation led by the decadent Western culture and

[1] Prince Nikolai Sergeevici Trubetsko was born in 1938 as part of the princely Lithuanian family of Trubetskoi. He was a linguist, his greatest contribution to this field being the development of structural linguistics.

[2] Petr Savitskii, born in 1895, was a geographer and economist. He graduated from the University of Sankt Petersburg, but after the Bolshevik Revolution, he immigrated to Sofia and later, to Prague.

[3] Georgii Florovskii, born in 1979, was a theologist and a philosopher. He immigrated to Paris in the 1920s and later to the USA, countries in which he held positions within academic institutions of the Orthodox Church.

[4] Born in 1887, George Vladimirovich Vernadsky was a naturalized American citizen who held multiple positions within Yale University, after spending a few years in Prague, where he met and exchanged ideas with the other Europeanists.

civilization" (Savitsky, 1925). Moreover, this territory is meant to be one political entity, undivided by borders, as Savitsky himself affirms: "The nature of the Eurasian world is minimally favourable to any sort of 'separatisms,' be they political, cultural, or economic." (Savitsky, 1934) In Savitsky's opinion, this situation occurred due to the heterogeneous distribution of resources within this space, which forced the different populations to interact and eventually merge together (Savitsky, 1934). On the other hand, both European and Asian populations have not been subjected to such conditions, which has led to the development of "statal" entities that control a relatively small geographical area (Savitsky, 1934).

As Eurasianists considered History and Geography to be fundamentally intertwined, this idea is closely tied to the concept of "mestoravitie" [development of a place], defined as "a certain geographic environment, which imprints the mark of its uniqueness on human communities which develop in that environment" (Vernadsky, 1927, p. 102). The Eurasian identity was thought to be the result of the existence of such a "mestoravitie" that encompassed the territories controlled by the Tsarist Empire or the USSR. As a result, the expansion of Moscow's control over foreign territories was considered a natural phenomenon, the adaptation of the inhabitants of the "mestoravite" to the specific characteristics of the geographical area they lived in (Titov, 2005). Thus, the Eurasian view of the Russian identity is noticeably broad, encompassing all the citizens of the Tsarist Empire, opposing the international movement for the self-determination of peoples which led to the creation of numerous new states and the disintegration of the European empires.

One noteworthy idea developed by the Eurasian scholars is the concept of "ideocracy" – the utopian way of organising the state that can only be achieved by the Eurasian civilization. This regime makes no difference between the citizens of the state based on religion or ethnic background, everyone being linked by a common historical destiny, and the ideas and wishes of the population are unitary and in perfect concordance with the decision of the state apparatus. However, in order for this perfect state to be achieved, the citizens have to give up their personal and familial interests and dedicate themselves to the state completely (Savitsky, 1925). Of course, this utopia is unachievable in any society, as each and every citizen has their own wishes and needs that

usually diverge from one another, so "ideocracy" is nothing but a façade for an oppressive regime.

During the Communist period, the main Eurasian author was Lev Gumilev, whose writings circulated mainly through clandestine canals during the period of the USSR. Gumilev adopted Vernandsky's idea of "mestorazvitie" [the concept of "place-development" or "topogenesis"], and considered that the Eurasian people should be encompassed within one great state (Gumilev, 1990). However, compared to his predecessors, his work focuses more on the scientific aspects that found his theories than on the ideological facets of the theory, such as the idea of the special destiny of Russia. Also, he introduced a new concept that of "positive Komplimentarnost" – the affinity between two cultures that facilitates their merging within the "mestorazvitie", in this case that of the Slavs and the peoples of the steppe (Titov, 2005).

Thus, it becomes clear that one of the main traits of the Eurasian theory that has remained a focal point from the classical Eurasianists to Gumilev is the all-encompassing view of the Russian identity. If Europe and Asia are composed of multiple ethnicities that generate multiple states, the Eurasian "mestoravitie" has to be included into one single state. This idea aligned with the expansionist tendencies that the Russian state has manifested all through modern history, a tendency that for the Empire meant the physical expansion of borders and for the USSR, enlarging its sphere of influence in order to become the most powerful state in the world and the winner of the Cold War. However, this definition of what is a Russian that focuses more on territory than on ethnicity, predates the birth of Eurasianism by centuries and can be best understood by examining the expansion of the Tsarist Empire (Tishkov, 2009). Starting from the fifteenth century, the Russians conquered other territories, inhabited by different ethnicities, thus expanding the borders of their states. The same tendencies were manifested by other European states as well, such as Great Britain or Spain that became veritable colonial empires. However, what set The Tsarist Empire apart was that there was no ocean separating the capital from the conquered territories. As a result, there was no clear distinction between the territory that constituted the heart of the Empire and what was the periphery, a fact that profoundly impacted the development of the Russian national identity (Petersson, 2020, p. 3). In time, it became hard to distinguish

between a member of the Russian ethnicity, called "ruskii", and one of the Russian state, the "rossians", a fact that led to the defining of a Russian through three characteristics: the loyalty towards the Tsar and the Empire; the Orthodox faith; and the use of the Russian language (Tishkov, 2009).

The fall of the Soviet Union meant not only the end of the Cold War, but also the end of Moscow's status as the capital of a global super-power. Having been bested by the United States and confronted with a major crisis on multiple levels, the Russian state could no longer exert its influence as it had done in the prior decades. During this time, multiple thinkers turned their attention to the Eurasian writings, adopting some of their ideas. Although such ideas had been conveyed in Russian far-right circles since the early 1990's, the Neo-Eurasian current of thought emerged during the mid-1990's, with Aleksandr Dugin being the main figure of this movement, which he remains until this day. A main difference between the Eurasianism of the twentieth century and Neo-Eurasianism is that the second current is actively trying to influence politics, as a Eurasian political party was formed in 2002 (Woo, 2022), while Dugin became part of president Vladimir Putin's inner circle.

Aleksandr Dugin's[5] interest for the right-leaning ideas manifested early, as he became part of an intellectual group from Moscow that focused not only on right-wing ideas, but also on more occult themes, such as mysticism and paganism (Dunlop, 2004). During this time, Dugin came into contact with multiple works of far-right thinkers from all around Europe that he was tasked with translating, such as Julius Evola, an Italian philosopher of pagan-fascist orientation. During Gorbachev's presidency, he became the leader of an anti-Semitic organization called Pamyat (Ingram, 2001, p. 3). In 1989, he travelled around Europe, strengthening ties with European leaders of the New Right movement, such as Alain de Benoist from France or Jean-Francois Thiriart, from Belgium, which are considered to be one of the main factors that influenced Dugin's later views on geopolitics (Dunlop, 2004). After the fall of the Soviet Union, he became a prominent writer, having his own

[5] Aleksandr Dugin comes from a long line of military men, his father allegedly having been a member of the Soviet secret service, the GRU.

publishing house[6], and publishing multiple works, the most prominent of which is *Foundations of Geopolitics* (Dunlop, 2004).

One of Dugin's main ideas that of the fight between the righteous East and the degenerate West, was also a focal point of the classical Eurasian writings, but now is interpreted in a fundamentally different manner. In Dugin's view, the main antagonist the Eurasian people have to fight against is not Europe, but the space of Anglo-Saxon Atlantica, a territory controlled by the United States and the United Kingdom (Dunlop, 2004). He sees these two spaces in contrast, with Eurasia being an earth-based empire, while Anglo-Saxon Atlantica is a sea-based empire. In Dugin's opinion, earth-based empires respect the differences between cultures and ethnicities, while Sea-based ones do no such thing, which explains the tendency of the United States to forcefully impose the American societal model over the cultures it has influenced over. However, Dugin does not view the whole of Europe as an enemy, the central and Eastern countries being potential allies in the upcoming fight against Anglo-Saxon Atlantica (Dugin, 2017). Also, Dugin's interpretation of the physical borders of the Eurasian space is different, as he advocates for the Russian expansion beyond the old borders of the Tsarist Empire and the Soviet Union, in order for Russia to be strong enough to counteract the Atlantic influence. In a post from 2014 on VKontakte, also known as VK, a Russian social media network, Dugin stated that the collapse of the Tsarist Empire happened because of Tsar Nikolas the Second's inability to conquer new territories and that an unstable, paranoid leader is good for a country as long as the state expand over new territories (Dugin, 2014).

Regarding the way Russia should be led, Dugin created the concept of the "state in depth", reminiscent of the "ideocracy" conceptualized by the Eurasianists of the 1920's and 1930's. This idea refers to the fact that the state should identify with a small portion of the elite, composed of experts in multiple domains that understand the true nature of statality, and the needs and objectives of the country should be more important than those of the citizens (Dugin, 2013).

[6] Arktogeya is the name of Dugin's Publishing House, a name borrowed from a German racist writer that combines the Greek words for "north" and "earth".

Identifying Neo-Eurasian influences on Russian strategic documents

Although Dugin's ideas have been regarded as inconsequential in the first decade of the twenty-first century, they have become more and more influential after the beginning of Vladimir Putin's third term as president in 2012, and even more so after the annexation of Crimea in 2014 (Kurt 2023).

The last ten years have been marked not only by military conflicts between Moscow and Kyiv that led to the invasion of Ukraine in 2022, but also by continuous informational attacks orchestrated by the Russian Federation against Ukraine and the Western world. In the following part of the paper we aim to highlight the way Dugin's Neo-Eurasianist ideas influence the strategic communication of the Russian Federation.

One of the main ideas promoted by the Russian Federation is that of the fight against the West. Although some measure of conflictuality undoubtedly exists, the Russian view is that this situation arose as a result of the unprompted hostility of the West against Moscow, such as the strategic documents released by the Kremlin or the official interviews of president Vladimir Putin, which will be analysed later. The aim of these actions is to inhibit its rise as a global power, so as not to threaten Washington's status as the main centre of geopolitical power (Rodkiewicz, 2023). In accordance with the Neo-Eurasian doctrine, the Occidental world is seen as degenerate, poisoned by modern culture, with Russia being the sole keeper of the traditional, Orthodox values (Dugin, 2017).

This idea is clearly visible in the strategic documents released by the Government of the Russian Federation since the annexation of the Crimean Peninsula (Składanowski, 2023, p. 2), which serve a double purpose: on one hand, they outline the main matters Russia is going to dedicate resources to within the following years, but on the other hand, they state the values and ideas the Russian government adheres to, which makes them indispensable for the building of a strong narrative.

In the Russian *National Security Strategy* of 2015, "the West" is painted as a unitary entity, which is one of the main threats to multiple facts of the Russian national security, intentionally acting against Russia through political and military means. For example, Russia frames every

NATO military exercise as a threat to its national security, an idea which developed into a full-scale disinformation campaign in the context of the "Spring Storm 21" exercise (EUvsDisinfo, 2021). Also, in 2021, an article on the Italian Sputnik website claimed that the European Union implemented economic sanctions against the Russian Federation because of a rusophobic lobby within the Union (EUvsDisinfo, 2021a). The National Security Strategy clearly states that the expansion of the North Atlantic Treaty Organisation towards the Russian border is a threat to the military security of the state (*Russian National Security Strategy*, 2015, art. 15). Moreover, the events that happened in Ukraine in 2014 are classified as an "anti-constitutional *coup d'etat*" (*Russian National Security Strategy*, 2015, art. 17) supported by the West that has generated a great amount of instability and suffering in the Ukrainian state. The process of "Eurasian integration", though not comprehensively explained within the strategy, is regarded as an integral part of achieving cultural security (*Russian National Security Strategy*, 2015, art. 81), but this process is hindered by the actions of the West. The Strategy also enumerates the "Traditional Russian spiritual and moral values," such as "the priority of the spiritual over the material", "service to the homeland" or "the historical unity of the peoples of Russia", cataloguing them as assets of cultural security (*Russian National Security Strategy*, 2015, art. 78). If this document acknowledges the existence of an Ukrainian state, its successor, the *National Security Strategy of 2021*, denies the rightful existence of an Ukrainian state, only talking about "the Ukrainian People" (*Strategy of the National Security of the Russian Federation*, 2021, art. 100), which aligns with the Eurasianist theory of a borderless "mestoravitie" (Vernadsky, 1927, p. 102). Moreover, the West is explicitly accused of trying to maintain world domination, as "The desire of Western countries to maintain their hegemony" (*Strategy of the National Security of the Russian Federation*, 2021, art. 7) is catalogued as one of the main trends that characterize the actual geopolitical climate.

The idea that certain entities wish to harm Russia is present through the mention of "The desire to isolate the Russian Federation and the use of double standards in international politics" (*Strategy of the National Security of the Russian Federation*, 2021, art. 18), which inhibits Moscow's ability to properly establish international relations.

After the invasion of Ukraine in 2022, the Russian official discourse started to rely in an even heavier manner on Dugin's Eurasian ideas regarding the Messianic character of the Russian people and the malevolent nature of the West, a situation made clear through the *Concept of Foreign Policy* of 2023. This document invokes the narrative of the thousand-year-old state in the first chapter, which is one of the main factors that determined **"**Russia's special position as a unique country-civilization" (*The Concept of the Foreign Policy of the Russian Federation*, 2023, art.4).

The states that pose a threat to the Russian Federation are referred to as "the United States of America (USA) and their satellites" (*The Concept of the Foreign Policy of the Russian Federation*, 2023, art.13), which aligns with Dugin's view that the United States are the main centre of power within the Anglo-Saxon Atlantic area.

The conflict in Ukraine is considered the result of the machinations of the Occident, aimed at deterring Russia from its path to the status of global power, so as to maintain "Western hegemony" (*The Concept of the Foreign Policy of the Russian Federation*, 2023, art.13). According to the Russian President, the West has pressured the Ukrainian state in order to weaken its economic ties with Moscow – "U.S. and EU countries systematically and consistently pushed Ukraine to curtail and limit economic cooperation with Russia" (Putin, 2021). In the same article, Vladimir Putin proposes a history of the Ukrainian and Russian states that justifies the idea that these two peoples should be part of the same "statal" entity. The name of the Ukrainian people comes, in the President`s view, from the Old Russian word for border ("okraina"), which was used in the twentieth century to refer to the Russians that lived close to the border of the state. The idea of a Ukrainian state appeared at the beginning of the nineteenth century, in the context of geopolitical unrest in the area. This idea was promoted by the Polish elite and during the First World War, by the Austro-Hungarians, which used it to counterbalance the Polish national movement. The article states that there are no cultural or ethnic reasons why the Ukrainian state should exist and this situation is the result of the manner in which the Soviet Union was organised. Today, any action of the Ukrainian people that tries to distance itself from the Russian identity is portrayed as a result of

Western interference that has to be counteracted for the good of the Russian and Ukrainian citizens. (Putin, 2021)

The same anti-Western narrative can be observed in the official discourses of the Russian president, with one of the most recent being the Victory Day speech from May 9th 2025, the day that marks the anniversary of the end of the Second World War for the USSR. With this occasion, Putin invokes the success of the USSR over Adolf Hitler's Third Reich. That anti-Western characteristic is clearly visible through the parallel drawn between the Western countries that act today in a manner that endangers Russia's national identity and the Nazis. Putin directly accuses the leaders of Europe for imposing their will on Ukraine "the elite in the West, they keep talking of their exceptionalism, of how they are different, and they are the ones creating a sense of disruption between our people" (Putin, 2025), in order to weaken Russia and maintain the status of the West as the centre of international power.

Channels of influence and mechanisms for propagating Eurasian ideology

Russia opts for a combination of soft-power and hard-power elements in order to propagate Eurasian ideals and undermine public trust in the capabilities and principles of Western powers. Soft power – also known as co-optive power – is the ability of a country to get "other countries to want what it wants", while hard power – or command power – is the ability of a country of "ordering others to do what it wants" (Nye, 2023, p. 12).

The neo-eurasianism finds practical expression in Moscow's policies toward the so-called "near aboard", namely the post-Soviet space, and the protection of Russian compatriots, initiatives that emerged during Vladimir Putin's second presidential term (2004-2008) and can also be interpreted through the conceptual framework of soft power. Also, in this context, the concept of the "Russian World" (Russkiy Mir) emerged, which is actually a soft security strategy aimed at "protecting" all Russian speakers outside the Federation. Following the Colour Revolutions in Georgia (2003), Ukraine (2004) and Kyrgyzstan (2005), as well as insignificant support from the population of Moscow's traditional allies, such as Kazakhstan and Belarus.

Russia has intertwined the Eurasianist ideology with soft power instruments in order to improve its international image and increase its attractiveness among the CIS states (Sergunin and Karabeshkin, 2025, p. 349). Thus, the following presents the main tools used, as well as the operating mode adopted by the Kremlin in the process of consolidating soft power.

The propaganda media apparatus is one of the Kremlin's main soft-power tools and is made up of various channels, including state-funded media outlets such as RT and Sputnik, multilingual multimedia platforms, and an active social media presence, to convey messages tailored to each country's culture and language (Wilson, 2015). The goal is not persuasion, but the creation of moral and factual confusion by multiplying versions of reality, so that the target audience loses its "cognitive basis for making political decisions" (Makhashvili, 2017), becoming passive and easy to manipulate. This tactic is compared by the specialized literature to the Soviet "4D" strategy: to discredit, to distort, to distract and to demoralize. However, its "post-modern" variant aims to reinvent reality (Makhashvili, 2017).

Since, in the vision of neo-Eurasianism, Russia is invested with a messianic mission to unify the Eurasian space into a single empire led by a single ruler, the Kremlin seeks the integration of all the states of the former USSR, as well as the extension of Russian protection over Eastern Europe (Zeyliger, 2025, p. 6) Thus, the countries of the post-Soviet space are the main targets of Eurasian propaganda. For example, in Belarus, Russian channels dominate the media space, and 62.3% of the population perceived the annexation of Crimea as "the return of historical lands." (Independent Institute of Socio-Economic and Political Studies, 2015). In Armenia, although trust in Russia declined after the Nagorno-Karabakh War[7], the Russian press remains the main source of information, supported by the presence of "peacekeepers" troops (Asgarli, 2024).

[7] The Second Nagorno-Karabakh War (September-November 2020), precipitated a significant erosion of public confidence in Russia among Armenians. Despite Moscow's role in mediating the ceasefire agreement and deploying peacekeeping contingents, its non-intervention military assistance in support of its Collective Security Treaty Organizations (CSTO) ally – Armenia – resulted in widespread accusations of failing its security guarantor role against Azerbaijan.

In Georgia, Russian propaganda exploits the popularity of Russian TV channels, such as Channel 1, RTR or Russia 1, due to the fact that the inhabitants are Russian speakers, but also the lack of access to local media in some regions, which explains why 30% of the minority population supports a pro-Russian orientation (National Democratic Institute, 2016). In Azerbaijan, Russia's influence is weaker, due to cultural proximity to Turkey, but there are still 340 schools teaching in Russian and the authorities avoid directly contradicting Moscow (Asgarli, 2024, p. 90). In Central Asia – Kazakhstan, Tajikistan, Turkmenistan, Kyrgyzstan, Uzbekistan – considered Russia's "backyard," cultural and linguistic dominance remains evident, even if in some regions there are nationalist manifestations (Asgarli, 2024, p.88).

In order to disseminate its narratives, including those regarding Eurasianism, to the widest possible audience, Russia also uploads propaganda content to social networks. It has been observed, since 2019, that Russian propaganda has also expanded among social media platforms, such as Facebook or Twitter (X), which are infested with messages such as "The Soviet Union was a politically stable and socially protected system" (Kintsurashvili and Gogoladze, 2020). Russia has developed a series of strategies over time to increase the visibility and credibility of pro-Russian content. Thus, in the context of sanctions suffered by the Kremlin, as well as the blocking or limiting of access to networks such as Facebook, Twitter (X) or YouTube[8]Russia has reoriented itself to Telegram in order to communicate with both external and internal audiences, due to the difficulty that the authorities face in trying to control the application. The Kremlin took advantage of the lack of a native recommendation mechanism, exploiting the platform's vulnerabilities through well-known influencers, such as Vladimir

[8] LinkedIn was officially blocked in 2016 for non-compliance with local data storage laws concerning Russian citizens. Access to Twitter (now X) became restricted starting in 2022, officially citing violations of Russian legislation regarding the dissemination of "fake news" related to the war. The most severe restrictions targeted Facebook and Instagram, which were officially banned in March 2022 after Meta was designated an extremist organization. The limitation of YouTube was primarily achieved through deliberate bandwidth throttling by the Roskomnadzor agency, rendering the platform nearly unusable without the aid of a Virtual Private Network (VPN) (https://russiapost.info/society/social_media_in_Russia).

Soloviev, who became "recommendation engine" for smaller accounts (Vavryk, 2022). Soloviev's recommendations increased channel views by up to 70% in the first few months, which also had a negative effect on larger channels. Users are generally attracted to small or medium-sized accounts that post original content with moderate frequency, and the Russian propaganda system monitors these preferences, constantly adjusting its strategies in a way that allows it to gradually remove channels that become irrelevant (Vavryk, 2022). In the broader context of information warfare campaigns deployed across media landscapes, analysts point to pro-Russian media outlets operating within the territories of former Soviet States. In Georgia, for instance, the propaganda system is also supported by the media through the portals Sakinformi, Sakartvelo da Msoplio, Iverioni and the publications Asaval Dasavali, Newspaper Alia or Svobodnaia Gruzia (Makhashvili, 2017). Pro-Russian narratives have also been promoted with the help of vocal personalities, such as Nino Burjanadze and Irma Inashvili (Makhashvili, 2017).

Another strategy developed by the Kremlin is determined by the emergence of a new stage, namely the Kremlin troll and the development of the Internet Research Agency (IRA), established in 2013[9]. Although it is currently no longer officially active, the organization is widely known, reaching over 600 employees, each with a daily technical sheet. Some of the workers were engaged in direct trolling by publishing and supporting propaganda messages on social networks, through comments and artificial discussions. Their goal was to attract users' attention to the topics and create the illusion of a popular consensus. The rest of the employees created apparently apolitical blogs and accounts, and gradually inserted messages pro-Russian interests. The agency carried out its activities on popular platforms such as LiveJournal, Vkontakte, Facebook, Twitter and Instagram, as well as in the comment sections of

[9] The IRA is a Russian organization, created, managed and financed by Yevgeny Prigozhin, focused on conducting online influence operations in order to manipulate public opinion. The agency gained notoriety for its involvement in the 2016 US Presidential election, the Brexit referendum and the ongoing war in Ukraine. Although the agency is no longer officially active under this name, having been publicly exposed and sanctioned internationally, its activities have been decentralized into less visible structures, allowing the continuation of the online manipulation campaigns.

news sites (Morrison, 2021). Even though the IRA is the only known such agency, there are researchers who believe that it exists as "an effective distraction from the wider network of troll farms, or the organization behind them" (Giles, 2016, p. 45). Typical of Kremlin propaganda, Eurasianists flood the media space with messages created and multiplied by "troll farms" (Gerber and Zavisca, 2016, p. 79).

Also, the Russian Orthodox Church is not only a key aspect of the Eurasian identity, as previously mentioned, but also "one of the main assets of Russia's soft power", but "foreign counteragents are frightened by it even more than by traditional leverages" (Lukyanov, 2009), therefore, it is also one of the main channels for the dissemination of Eurasian ideas. Russian propaganda promotes principles such as "Moscow is the third Rome" or "Holy Rus" which induce the idea that the Moscow Kingdom, and later Russia, is the spiritual successor of Byzantium, being the true "citadel of Orthodoxy" (Balatska, 2023, p. 127). Russia is considered the sacred source of the "correct" faith, which has the mission of spreading it to other peoples. Furthermore, according to Eurasianism, being "Orthodox" is equivalent to being "Russian", and thus, any Orthodox community is considered part of the "Russian World" (Balatska, 2023, p. 127). In this way, two distinct elements of collective belonging – religion and ethnicity – are combined, causing confusion at the level of identity (Balatska, 2023, p. 127). For example, propaganda in the Georgian space includes the demonization of the EU and NATO, which are presented as threats to the identity, value and the Orthodox Church, while Russia is portrayed as an ally and protector of Georgia (Makhashvili, 2017).

On the other hand, in promoting the Eurasian ideology, the Russian Federation also uses a series of institutional actors, including think tanks and quasi-governmental organizations, the latter being known as GONGOs (Government-Organized Non-Governmental Organizations). Think tanks are institutions that conduct analysis and research, acting as a bridge between academia and politics, while GONGOs are organizations that, although presenting themselves as non-governmental, are created and controlled by the government (Pallin and Oxenstierna 2017). In a study conducted by Denis Yu. Ivanov, in which he analyses the research directions of seven analytical centres specialized in the field of political

studies in the Eurasian space, it is noted that the theme of "Greater Eurasia" represents a priority for institutions with a strategic and geopolitical profile (Ivanov, 2023).

"Greater Eurasia" is part of a series of concepts that "describe and form the so-called political images of the world," along with some political initiatives as Shanghai Cooperation Organization (SCO), BRICS, One Belt, One Road (OBOR) or the Community of Shared Future for Mankind (Bazavluk, Kurylev and Savin, 2022). The concept was defined in 2015, although it has been a topic of interest before, and Sergey Karaganov, founder of the Council on Foreign and Defence Policy, views it as "a movement towards a new geostrategic community – a pan-Eurasian space of development, peace and security, intended to overcome the divisions left over from the Cold War, to prevent the emergence of new ones, to manage misunderstandings and frictions" (Karaganov, 2018). Thus, the Council for Foreign and Defence Policy[10] shows a particularly high interest in this concept, producing 98 publications in the period 2014-2023 on this topic. It is followed by the Foundation for World Policy Research, whose main interest focuses on the "Greater Eurasia", considered an integrative image of the world (Ivanov, 2023).

Another channel used to propagate Russian narratives is pseudo-think tanks, which are organizations that emerged as proxies of the Kremlin "that blur the lines between news, think tank content, misinformation, and propaganda" (Williams and Carley, 2023, p. 3). According to Williams and Carley (2023), the role of pseudo-think tanks is to disseminate pro-Russian propaganda to the Western public, and, according to their research, their credibility and visibility are increased through an artificial boost process through a network of low-quality websites, which generate millions of backlinks to these platforms. Among the examples identified by the two authors are: Global Research

[10] The Council on Foreign and Defence Policy (CFDP/ SVOP) is an influential, semi-official think-tank established in Moscow in 1992, and serves as a principal provider of strategic consultancy on Russia's foreign and defence policy issues. Due to its institutional role and the presence of Karaganov Sergey as its Honorary Chairman, the CFDP is pivotal in the conceptual development and ideological promotion of the "Greater Eurasia" project.

(globalresearch.ca), Strategic Culture Foundation (strategic-culture.org), New Eastern Outlook (jurnal-neo.org), Geopolitica.ru (geopolitica.ru-en), SouthFront (southfront.org), Katehon (Katehon.com-en), en.news-front.info (Williams and Carley, 2023) (Williams and Carley 2023).

Moreover, organizations such as the Eurasian Economic Union (EAEU), the Commonwealth of Independent States (CIS), the Collective Security Treaty Organization (CSTO) and the Shanghai Cooperation Organization (SCO), or initiatives such as The Greater Eurasia Project/ Greater Eurasian Partnership, are considered instruments through which Eurasian ideas are implemented, as Russia's strategies to become a pole of power independent of the West by creating a multipolar world order (Bazavluk, Kurylev, and Savin, 2022). For example, the EAEU was established without being based on a common system of ideas, and a number of leaders such as Nursultan Nazarbayev and Sergey Glazyev supported the adoption of Eurasianism as the organization's ideology, but member states oriented towards cooperation with the West opposed it (Pantin, 2022). However, Russia, as the core state of the EAEU, continues to promote the principles of Eurasianism, seeking to expand its influence beyond the economic sphere and proposing an ideological formula structured in the form of a triad – "peace and security, human capital, support points" (Pantin, 2022). In practice, the Kremlin wants to portray the EAEU as a "third way" between Western liberalism and Chinese socialism (Kharitonova, 2024). This is also supported by pro-Russian authors, such as V. I. Pantin who believes that "Eurasianism, if developed and adapted to modern realities, can ensure stronger economic integration" and that it is necessary to "overcome illusions regarding the possibility of integration into the EU" (Pantin, 2022, p. 17). Also, S. Yu. Glazyev and I.F. Kefeli proposes "an ideology of Eurasian integration that would express not only economic interests, but also common socio-political and spiritual interests" (Glazyev and Kefeli, 2022, p. 10). For example, in Georgia there are a number of organizations involved in the dissemination of Eurasian narratives, including the Eurasian Institute – which carries out analytical and outreach work through conferences and seminars – and Eurasian Choice – which organizes social actions, protests and demonstrations, both of which have direct or indirect connections to the International Eurasian

Movement, which is led by Aleksandr Dughin. Around them revolve a number of associated entities, such as the Young Political Scientists Club, the People's Movement of Georgian-Russian Dialogue and Cooperation, the Erekle II Society, Patriot TV (Makhashvili, 2017). The activity of these pro-Russian organizations in Georgia during the 2008 Russian-Georgian conflict represented a testing ground for the strategies that the Russian Federation uses in information warfare, the "propaganda machine" being used on a large scale for the first time.

In parallel, in order to maintain its influence over the former Soviet republics, the Kremlin created a constitutional[11] clause on the protection of "compatriots" living outside Russia's borders, which stipulates the protection of Russian rights, interests and cultural identity (Ministry of Foreign Affairs of the Russian Federation, 2020). This vague formulation provides the Russian Federation with a justification for its interventions in its "near neighbourhood", under the pretext of securitising the "Russian world" (Asgarli, 2024). In the same context, the policy of issuing Russian passports to the populations of the separatist regions of the former USSR was also created. Thus, citizens of Transnistria (Republic of Moldova), Abkhazia and Ossetia (Georgia), as well as the Ukrainian territories of Donbas, Kherson, Luhansk and Zaporizhia received Russian identity cards, even though some of them did not express a desire to become Russian citizens (Asgarli, 2024). These actions had served to legitimize the military interventions – namely the hard power elements – that Russia has carried out over time in these regions. Among the Kremlin's aggressive steps, we recall: involvement in the conflict between Armenia and Azerbaijan since the end of the Soviet era, granting support to Armenia in 2020, conditional on abandoning negotiations with the European Union and joining the EAEU and stationing Russian forces in Karabakh, supporting the separatist republics of Abkhazia and Ossetia, the Russian invasion of Georgia in 2008 (Bantaş and Bălănică, 2023).

[11] The provision is Article 69, Paragraph 3 (Art.69, Sec.3) of the Constitution of the Russian Federation, a clause included in the context of the constitutional amendments added in 2020 through which Kremlin sought to adjust the balance of power and adapt the fundamental law to the new reality, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651935/EPRS_BRI(2020)651935_EN.pdf.

Case Study: The War in Ukraine through the Lens of Eurasian Ideology

The invasion of Ukraine by Russia on February 24, 2022, is itself a geopolitical and ideological manifestation of Eurasianism, the Russians claim the Kyivian Rus as the cradle of Russian civilization, the territory around Kyiv being a key point of their identity as a thousand-year-old independent state (Balatska, 2023, p. 2). The loss of the Ukrainian territory as a result of the dissolution of the Soviet Union has meant, from an ideological point of view, the loss of that identity, which dealt a powerful psychological blow to the inhabitants of the newly-formed Russian Federation. Today, the Neo-Eurasian school of thought promoted by Dugin relies on the idea that Kyiv and the territories that surround it are an integral part of the Eurasian space, which means they have to be encompassed again within the area controlled by Moscow (Dughin, 2015). This fact is evident even from the ideologue's statements, "For its greatness, Russia will pay with bloodshed" (Dughin, 2015, p 1) and "Sacred war for sacred order will rescue the current world [from] its darkest place" (Dughin, 2023, p 11).

In the Eurasian perspective, Ukraine is part of the Russian state, and "the Little Russians have been 'one of the individuations of the Russian people' along with the Great Russians and Belarusians (Balatska, 2023, p. 131). As experts stressed, Dughin argues that Ukrainian identity did not develop naturally, but was manufactured by Western states (Kurt, 2023, p. 361), and that Ukraine's sovereignty and independence represent a "highly adverse condition" for Russian geopolitics and a significant threat to the integrity of Eurasia (Kurt, 2023, p. 360). Furthermore, the ideologist believes that Ukrainian territory is easily divisible between Russia and the USA. The loss of Kiev, considered to be "the first Russian state", represents "a vital geopolitical setback for the Russian state", which not only affected Russia's foreign policy and geostrategic options, but also created "the most acute psychological and ideological problems" (Balatska, 2023, p. 124-125).

The solution to the so-called "Ukrainian question", as promoted by propaganda machine, is exclusively military (Dugin, 2000, p. 86) and the annexation of Crimea is considered an essential stage for Russia's return as a global power and for securing access to the Black Sea, and the

events of 2014 have been catalogued as the "sacrificial awakening" of Russia. Dugin's Neo-Eurasianism proposes a phased plan to conquer Ukraine, firstly commencing with the geopolitical announcement represented by the capture of Crimea, step followed by the "collection of the Russian Empire", focusing on the eastern and southern parts of Ukraine, which would serve as a base for mobilization and recruitment. Ultimately, the plan aims at the unconditional military solution, leading to the re-division of Ukrainian territory and the extermination of the Ukrainian ethnos (Dughin, 2015). This war is legitimized as a "civilizational war" aimed at ensuring the survival and consolidation of Eurasian civilization, and the territory of Ukraine is considered indispensable for the achievement of "Russia's historical mission" (Zeyliger, 2025). Moreover, experts highlight that Dugin also points out that during the Leninist Soviet regime, the Ukrainian Soviet Socialist Republic was artificially united from regions with distinct histories and ethnicities (Kurt, 2023, p. 361). Thus, the myth of the "disintegration of Ukraine" is a central element of the anti-Ukrainian discourse of Eurasianism, but also of some internal political forces, such as the Progressive Socialist Party, the Communist Party, the Union of Left Forces, and the Party of Regions (Balatska, 2023, p. 139).

Eurasianists are trying to exploit the identity division at the level of Ukrainian society in order to destabilize the state. The societal rupture is highlighted by the contrasts between the east and the west of the country. A correlation is observed between the spoken language, religious affiliation and political options, so that in the west and centre, ethnic Ukrainians, speakers of the official language, supporters of strengthening relations with the West and followers of the Ukrainian Orthodox Church of Kiev Patriarchate predominate (Rațiu and Munteanu 2018, p. 194). In parallel, in the east and south of Ukraine, ethnic Russians are the majority, who communicate in Russian, support the intensification of relations with Russia and are affiliated with the Ukrainian Orthodox Church of Moscow Patriarchate (Rațiu and Munteanu 2018, p. 194). Also, in this sense, the political and social crises of 1994, 2004 and 2013-2014 were reinterpreted by pro-Russian propaganda as evidence of a "civilizational cleavage", and the map created by Timofey Sergeytsev, which divided the population of Ukraine into three degrees, emphasized

the artificial idea of a fragmented and unstable nation (Balatska, 2023, p. 139). However, this "trend" reached its peak with the promotion of the "Novorossiya project", a historical name, by the Kremlin during the "Russian-Ukrainian" war, through which an attempt was made to legitimize a "quasi-state" made up of the southern and eastern regions of Ukraine – Dnipropetrovsk, Donetsk, Zaporizhzhia, Kirovohrad, Luhansk, Mykolaiv, Odessa, Kharkiv, Kherson regions and the Autonomous Republic of Crimea (Balatska, 2023, p. 140). In these regions, the Russian-speaking population predominates and since 2014 a media campaign has been launched to support "cultural and historical ownership of these regions by Russia" (Balatska, 2023, p. 140).

In 2014, the anti-Ukrainian propaganda centred on the "Zionist/ Khazar conspiracy" and hybrid labels such as the "Jewish-Banderist junta," with Ukrainian Jews, Freemasons, and nationalists paradoxically associated with the Nazis (Balatska, 2023, p. 141). However, with the invasion of 2022, the myth of "Nazi Ukraine" emerged, despite the Jewish origin of Ukrainian President Zelensky, who would be responsible for a so-called "genocide of the population of Donbas", considered the "genocide of the Russian people", which was the official reason for "denazification" (Balatska, 2023, p. 142).

Eurasian propaganda tends to demonize Ukraine, promoting fake news about "the spread in Kyiv of the "Thelema, liberal-satanic and Atlanticist sect" and obsessively assigning it labels such as "ukro-fascists", "neo-Nazis", "junta", "Banderists", "puppets of the West" (Balatska, 2023, p. 135-136). Moreover, in March 2022, T. Sergeytsev published an article entitled "What Russia Should Do with Ukraine" in which the Ukrainian people were entirely transformed into a "collective culprit", and "debanderisation" was transformed into "de-Ukrainisation," which implies the abolition of the state, culture and even the name "Ukraine", presented as an "artificial anti-Russian construction" (Balatska, 2023, p. 141-142).

As proof of the effectiveness of propaganda, domestically, President Vladimir Putin has managed to impose the narrative of a "special military operation" carried out for the purpose of "demilitarizing and denazifying" Ukraine, with the invasion being portrayed as a vital action for Russia's security (Asgarli, 2024, p. 88). The success of the discourse is highlighted

in the results of surveys conducted among the Russian population: according to the Russian Centre for Public Opinion Research (VCIOM), 78% of citizens say they trust Putin, and 68% support the "special operation" (Russian Public Opinion Research Centre (VCIOM), 2023). Even with a slight increase in scepticism after the second half of 2023, the majority of residents continue to legitimize the Kremlin's actions, with Statista recording a level of 75% in terms of population support (Asgarli, 2024, p. 88).

These Eurasian narratives are also found in the official speech delivered by the Russian Federation internationally, through the Russian President, Vladimir Putin. A clear example is the lecture given by Putin in Moscow, on 14.06.2024, at a meeting with the Russian Ministry of Foreign Affairs. He emphasizes that the crisis in Ukraine is not "a conflict between two states," but the result of aggressive policies of the West aimed at "dismembering our Motherland" (the former Soviet Union), Russians and Ukrainians being "united by a common history and culture, spiritual values, millions of family ties," more precisely by "Russian language, culture, traditions, historical memory" (The Ministry of Foreign Affairs of the Russian Federation, 2024). Putin accuses the West of trying to turn Ukraine into their "bridgehead", turning it anti-Russian by supporting neo-Nazi and radical groups. He claims that there were a series of pogroms, violence and crimes in Ukraine, and that the radicals who took power rehabilitated the Nazis, tried to "abolish the Russian language in the state and public sphere" and put pressure on Orthodox believers (The Ministry of Foreign Affairs of the Russian Federation, 2024). Putin also invokes Article 1, paragraph 2 of the UN Charter and the 2010 decision of the International Court of Justice on the status of Kosovo to legitimize the referendums held in the separatist regions of Donetsk and Lugansk: "If the West recognized Kosovo, then Donetsk and Lugansk have the same right." (The Ministry of Foreign Affairs of the Russian Federation, 2024). In addition, Russia is portrayed as the guarantor of the security of the Russian-speaking populations in Crimea and Donbas, with Russian troops having a "civilizational mission to protect the "Russian world" (Russkiy Mir)" (The Ministry of Foreign Affairs of the Russian Federation, 2024). In practice, the Kremlin assumes the role of protector of Russian-speaking communities, while

Kiev is presented as the aggressor who allegedly started the war against the "independent people's republics" (The Ministry of Foreign Affairs of the Russian Federation, 2024).

The myth of genocide is also propagated, with Putin declaring that in Donbass "terrorist attacks, murders were committed, a belly blockade was organized" and that women, children and the elderly were labelled as "second-class people, subhumans" (The Ministry of Foreign Affairs of the Russian Federation, 2024). In addition, Putin claims that he tried all political and diplomatic solutions through negotiations in Belarus, Turkey and Istanbul, invoking the "Treaty on Permanent Neutrality and Security Guarantees for Ukraine" as evidence of a possible compromise, but rejected by the "Bucha provocation" (The Ministry of Foreign Affairs of the Russian Federation, 2024).

The president also mentions that Russian troops approached Kiev only as a means of pressure for negotiations, not with the aim of conquering the capital. Last but not least, Putin proposes conditions for peace, through which he demands that Zelensky completely withdraw troops from Donetsk, Lungask, Kherson and Zaporozhye, but also to abandon the steps to join NATO, so that the neutrality, demilitarization and denazification of Ukraine are accepted (Ministry of Foreign Affairs of the Russian Federation, 2024). The discourse with Eurasian undertones continues today, so that at the 2025 Alaska Conference, Putin states that "we've always considered the Ukrainian nation, and I've said it multiple times, a brotherly nation" and that "We have the same roots, and everything that's happening is a tragedy for us, and terrible wound" (CBS News, 2025). Peace is also still conditioned by the fulfilment of Russia's "legitimate concerns" and the restoration of a "just balance of security in Europe and the world" (CBS News, 2025).

The invasion was also supported through social media, with the Kremlin trying to gain support from users by publishing propaganda posts and creating the illusion that there were many legitimate pro-Russian accounts. Moreover, Russia manipulated authentic footage from the front, presenting "Ukrainian atrocities" in order to create panic and erode support for Kiev (Peresypkina, 2025).

However, a famous example of material that pro-Russian propaganda used is the image of Anna Ivanovna, a 69-year-old woman of

Ukrainian origin, waving a red flag (Bettiza and Khomenko, 2022). The moment was transformed into a sign of nostalgia for the USSR period and of the alleged popular support for the Russian invasion, the woman being associated with the image of "Mother Russia". Her pose was transformed into a propaganda symbol, being multiplied through murals, statues, songs, poems and stickers, the old woman becoming the iconic figure of "liberating Russia". However, the case of "Babushka Z", as she was called, is a well-known example of distortion and narrative simplification, as the old woman does not support the Russian military operation, and when Anna was interviewed she stated: "How can I support my people by dying? My grandchildren and great-grandchildren were forced to go to Poland. We live in fear and terror" and that "If I could talk to Vladimir Putin, I would tell him that you made a mistake. We, the Ukrainian workers, what did we do to deserve this? We are the ones who suffer the most". Unfortunately, the woman is now being attacked online, and her neighbours are avoiding her, considering her a traitor (Bettiza and Khomenko, 2022).

In parallel with such posts, Russia is building its own user base through fake accounts and bots. In the early stages of the 2022 invasion, the Kremlin mobilized state television, troll farms, and bot networks to spread contradictory justifications for the "special military operation," ranging from "denazification of Ukraine" and protection of Russian-speaking communities to defence against "NATO encirclement" (Bronk, Collins, and Wallach, 2023).

The information campaign was also accompanied by cyber-attacks on Ukrainian government websites, which aimed to undermine trust in the authorities (Peresypkina, 2025). According to the study conducted in 2023 by Geissler et al., between February and July 2022, 349,455 pro-Russian messages were collected on Twitter (X), which generated almost 1 million likes and an audience of approximately 14.4 million users. These ranged from simple hashtags, such as #IstandWithPutin or #StandWithRussia, to state verbal affirmations of support for Vladimir Putin, such as "@RWApodcast I literally love Putin. The most honest leader in the world" (Geissler, Bär, Pröllochs, and Feuerriegel, 2023, p. 13). Bots also played an important role in the propagation of pro-Russian posts, with the analysis by Geissler et al.

showing that over 132,000 accounts spread the messages, of which approximately 20% were operated by bots. Moreover, a significant part of these accounts was created right around the invasion and played an essential role in amplifying the messages through retweets – approximately 25.7% (Geissler, Bär, Pröllochs, andFeuerriegel, 2023, p. 13).

The Russian information warfare strategy against Ukraine has unfolded through a series of distinct, adaptive phases. The first one – the Shock and Confusion phase - focused on minimizing the invasion as a "special operation" and denying atrocities. Starting with 2023 – the second phase, also known as the adaptation and recalibration phase – due to unexpected resistance from Ukraine, the propaganda reoriented, promoting narratives such as "Kiev fatigue" (Peresypkina, 2025). Taking advantage of the state's energy insecurity and the socio-economic costs of supporting Ukraine, Russian propaganda fuelled the discontent and fears that caused protests in countries such as Germany, France and Italy. Also, traditional tools like RT and Sputnik have gradually been replaced by indirect methods, such as proxy influencers, pseudo-independent press, and local sympathizers.

In the accelerated technological phase – the third one – of Russian propaganda and disinformation in 2024, deep fakes depicting Ukrainian officials "surrendering" or Western leaders denigrating Kiev were notable, going viral on platforms such as Telegram and TikTok, taking advantage of the low level of digital literacy of users (Krlis, 2024). Automated tools for "comment flooding" appeared and fake articles, fictitious "leaks" of NATO information, and fabricated reports of war crimes were published. Thus, Russia adopted a strategy called "spray and pray" (Niemien, 2024), through which it flooded the online space with huge volumes of apparently credible fakes, exceeding the capacity of fact-checkers. These efforts are countered by phase IV (2024-2025), which is focused on Resilience and strategic communication from Ukraine.

Finally, in phase V (2025), Russia is trying to weaken NATO unity, presenting Trump's return to the US presidency as a sign of a possible fracturing of the organization. The Kremlin is also trying to exploit divisions within American society, launching fakes on X or Truth Social about Trump's alleged recognition of Russian control over Ukrainian territories (Krasnodemska, Marchenko, Ostapchuk, and Sonechko,

2024). In addition, there is a tendency for Russia to insert propaganda content into restricted groups on Telegram, WhatsApp, or Facebook, so as to create discontent at the community level and be difficult to detect at the macro level (Peresypkina, 2025).

Conclusions

In conclusion, Neo-Eurasianism represents a revival of centuries-old ideas about the uniqueness of the Russian state that comes to strengthen the expansionist tendencies of Putin`s Russian Federation. Ideas belonging to this current have been influencing the strategic communication and propaganda campaigns coordinated by the Russian Federation since the re-election of president Vladimir Putin in 2012, a phenomenon that was intensified first by the events of 2014 and later by the full-scale Russian invasion of Ukraine in 2021. The discourse analysis has revealed that the recent Russian strategic documents, be they actual or recently replaced, that serve as coordinates of Russian state policy bear the mark of Neo-Eurasianism, as do the discourses and interviews of the President. The Russian narratives interpret the international stage through the lens of these ideas, which depicts the West as a hostile, rusophobic entity that has rejected the "true" values in order to maximize its financial gains and its influence over other peoples. In this narrative, the Kremlin is the sole keeper of these authentic, Orthodox values, its unique mission being that of protecting the neighbouring countries from the decadent Western influence. After 2021, the idea of the homogenous Russian population that is spread over the whole Eurasian space has made its presence felt through the denial of the existence of a Ukrainian people, as it can be seen both through the strategic communication and propaganda campaigns of the last four years.

Moreover, these ideas are spread through propaganda campaigns across multiple channels, both within and outside the borders of the Federation. This variety of channels aims to spread the propaganda message to all members of the society, as each of them has its own specificity and reaches a different segment of the population. The propaganda campaigns are used as a form of soft power aimed at increasing Russian influence over the neighbouring states. However,

when the soft power elements are not enough, the Kremlin does not shy itself from employing hard power as well. Regarding the war in Ukraine, it can be easily explained through the Neo-Eurasianist ideas upheld by Dugin. The "special military operation" is perceived as a necessity of the state, as the Eurasian and Neo-eurasian doctrines do not consider the Ukrainian territory as a separate country. In this regard, the propaganda machine targets the people inside the Russian Federation, in order to rally the population behind the war effort, and those outside the Russian borders, in a manner that would justify the military invasion. These two are branches of the same campaign, drawing inspiration from Dugin's ideas. As a result, the way Moscow positions itself in relation to Kyiv can be seen as an extension of the Neo-Eurasianist and Eurasianist ideas.

References:

1. Asgarli, T. (2024). "Russian propaganda – a tool for rebuilding the Soviet Union?" *Athenaeum. Polish Political Science Studies,* vol. 83(3), pp. 81–95.

2. Balatska, O. (2023). "Eurasianism, Neo-Eurasianism and Anti-Ukrainianism in the narratives of modern Russian propaganda." *Studia Polityczne*, *50*(4), pp. 123–148. https://doi.org/10.35757/stp.2022.50.4.03

3. Bantaș, D.-A., and Bălănică, S. (2023). "The actions of the Russian Federation from the perspective of individual responsibility." *Buletinul Universității Naționale de Apărare "Carol I",* 2/2023, April-June, pp. 105–119.

4. Bazavluk, S. V., Kurylev, K. P., and Savin, L. V. (2022). "Eurasianism, Eurasian Economic Union and Multipolarity: Assessments of Foreign Experts." *Vestnik RUDN. International Relations.* Vol. 22 No. 1, pp. 30–42.

5. Bettiza, S., and Khomenko, S. (June 15, 2022). *BBC*. Retrieved 08 20, 2025, from https://www.bbc.com/news/world-europe-61757667

6. Bronk, C., Collins, G., and Wallach, D. (2023). "The Ukrainian Information and Cyber War." *The Cyber Defence Review*. Vol. 8. Issue 3, pp. 33-50.

7. CBS News. (August 15, 2025). CBS News. Retrieved 08 20, 2025.

8. Dugin, A. (2017). *Foundations of geopolitics: The geopolitical future of Russia*: English translation.

9. Dugin, A. (2013). *The State in Depth*. MED. http://med.org.ru/article/4703

10. Dugin, A. (2014). *Alexander Dugin: Posts*. VK. https://vk.com/wall18631635?day=31122021&owners_only

11. Dunlop, J. B. (2004). *Aleksandr Dugin's Foundations of Geopolitics*. FSI. https://tec.fsi.stanford.edu/docs/aleksandr-dugins-foundations-geopolitics?utm_source=chatgpt.com

12. EUvsDisinfo. (May 17, 2021). *Disinfo: NATO exercises are a threat and provocation against Russia.* https://euvsdisinfo.eu/report/nato-exercises-is-a-threat-and-provocation-against-russia/

13. EUvsDisinfo. (May 2021a). *Disinfo: An aggressive Russophobic lobby within the EU is responsible for EU sanctions against Russia*. https://euvsdisinfo.eu/report/an-aggressive-russophobic-lobby-within-the-eu-is-responsible-for-eu-sanctions-against-russia/

14. Geissler, D., Bär, D., Pröllochs, N., & Feuerriegel, S. (2023). *Russian propaganda on social media during the 2022 invasion of Ukraine.*

15. Gerber, T. P., and Zavisca, J. (2016). "Does Russian Propaganda Work?" *The Washington Quarterly, 39:2*, pp. 79–98.

16. Giles, K. (2016). "Russia's 'New' Tools for Confronting the West. Continuity and Innovation." *Chatham House. The Royal Institute*.

17. Glazyev, S. Y., and Kefeli, I. F. (2022). "On the Question of the Ideology of the Eurasian Economic Union." *Eurasian Integration: Economics, Law, Politics,* 16(1), pp. 10–21.

18. Gumilev, L. N. (1990). *Ethnogenesis and the biosphere*.

19. Ivanov, D. Y. (2023). "Concepts of Political Worldviews of the Eurasian Space in the Communicative Practice of Think Tanks." *Eurasian Integration*, pp. 122–132.

20. Ingram, A. (2001). "Alexander Dugin: Geopolitics and neo-fascism in post-Soviet Russia." *Political Geography*, 20(8), pp. 1029–1051. https://doi.org/10.1016/s0962-6298(01)00043-9

21. Karaganov, S. (2018). "The new cold war and the emerging greater Eurasia." *Journal of Eurasian studies,* 9(2), pp. 85–93.

22. Kharitonova, N. I. (2024). "Search for the ideological basis of the EAEU. General integration and youth aspects." *Russia's State University for the Humanities (RGGU)*, pp. 77–88.

23. Kintsurashvili, T., & Gogoladze, T. (2020). *Anti-Western Propaganda*. Media Development Foundation.
http://mdfgeorgia.ge/uploads//antidasavlurieng2020_compressed.pdf .

24. Krlis, M. (2024). "The Information War: Russia-Ukraine Conflict." *Georgetown Journal of International*. https://gjia.georgetown.edu/2024/02/02/

25. Kurt, S. (2023). "An analysis of the motives of the Russian Federation–Ukraine war within Dugin's understanding of Neo-Eurasianism." *Codrul Cosminului,* XXIX, No. 2, pp. 351–374.

26. Lukyanov, F. (2009). "Poiski Myagkoy Sily." *Forbes Online,* 2 November. http://www.forbes.ru/column/.

27. Makhashvili, L. (2017). "The Russian information war and propaganda narratives in the European Union and the EU's Eastern Partnership countries." *International Journal of Social Science and Humanity 7(5)*, pp. 309–313.

28. Ministry of Foreign Affairs of the Russian Federation. (July 3, 2020). *The Constitution of the Russian Federation*. Ministry of Foreign Affairs of the Russian Federation (MID): https://mid.ru/en/foreign_policy/fundamental_documents/1750525/

29. Meyer, C. (2009). "Rostovtzeff and the classical origins of Eurasianism." *Anabases*, 9, pp. 185–197. https://doi.org/10.4000/anabases.419

30. Morrison, S. (2021). *Russian Information Operations.* PhD Thesis, Swinburne.

31. Nieminen, H. (2024). "Why Does Disinformation Spread in Liberal Democracies? The Relationship between Disinformation, Inequality, and the Media." *Journal of the European Institute for Communication and Culture.* Vol. 31. Issue 1, pp. 123–140.

32. Nye, J. S. (2023). "'Soft power'. Soft Power and Great-Power Competition: Shifting Sands in the Balance of Power between the United States and China." *Singapore: Springer Nature Singapore*, pp. 3–15.

33. Pallin, C. V., and Oxenstierna, S. (2017). *Russian Think Tanks and Soft Power.* Totalförsvarets forskningsinstitut (FOI).

34. Pantin, V. (2022). "The Ideological Foundations of Eurasian Economic Integration." *RUDN University Journal,* 22(1), pp. 17–29.

35. Peresypkina, I. (2025). "The Evolution of Russian Disinformation Strategies in the Context of the Russian-Ukrainian War (2022–2025)." *Mediaforum: Analytics, Forecasts, Information Management,* Volume 16, pp. 34-37.

36. Petersson, B. (2020). "Nationalism and greatness: Russia under the Putin presidencies." In *Research Handbook on Nationalism*. Edward Elgar Publishing. https://doi.org/10.4337/9781789903447.00041

37. Putin, V. (2025). *Putin delivers victory day speech transcript*. https://www.rev.com/transcripts/putin-delivers-victory-day-speech-transcript

38. Putin, V. (2021). Article by Vladimir Putin *"On the Historical Unity of Russians and Ukrainians"*.

39. Rațiu, A., and Munteanu, A. (2018). "Hybrid Warfare and the Russian Federation Informational Strategy to Influence Civilian Population in Ukraine." *Land Forces Academy Review Vol. XXIII, No 3(91)*, pp. 192–200.

40. Rodkiewicz, W. (2023). "An anti-colonial alliance with the Global South. The new 'Foreign Policy Concept of the Russian Federation.'" *OSW Commentary – Centre for Eastern Studies*, *1*(506).

41. *Russian National Security Strategy* (2015). https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf

42. Russian Public Opinion Research Centre (VCIOM). (2023). *Special Military Operation: A Year Later. Russian Public Opinion Research Centre (VCIOM).* Retrieved from https://wciom.com/press-release/special-military-operation-a-year-later.

43. Savitsky, P. (1925). "Eurasianism as a Historical Design." *The Foundations of Eurasianism*, 1(1).

44. Savitsky, P. (1934). "The Geographical and Geopolitical Foundations of Eurasianism." *Orient Und Occident*, 1(17).

45. Sergunin, A., and Karabeshkin, L. (2025). "Understanding Russia's Soft Power Strategy." *Politics,* Vol. 35(3-4), pp. 347-363.

46. Składanowski, M. (2023). "We Are No Longer Europeans: The evolution of the image of Europe and the West in Russian strategic documents (2007–2023)." *Gdansk Russian Studies*, *10*, pp. 179–189. https://doi.org/10.26881/srg.2023.10.12

47. *Strategy of the National Security of the Russian Federation* (2021). https://rusmilsec.blog/wp-content/uploads/2021/08/nss_rf_2021_eng_.pdf

48. *The Concept of the Foreign Policy of the Russian Federation* (2023). https://mid.ru/en/foreign_policy/fundamental_documents/1860586/

49. The Ministry of Foreign Affairs of the Russian Federation. (June 14, 2024). *President of Russia Vladimir Putin's speech at the meeting with senior staff of the Russian Foreign Ministry, Moscow, June 14, 2024*. The Ministry of Foreign Affairs of the Russian Federation: https://mid.ru/en/foreign_policy/news/1957107/

50. Tishkov, V. A. (2009). *The Russian People and National Identity*. *National Reconciliation, Inter-Ethnic and Inter Confessional Tolerance in the Balkans Reconciliation and Human Security*, 1(1).

51. Titov, A. S. (2005). *Lev Gumilev, ethnogenesis and eurasianism*. UMI Dissertation Publishing.

52. Vavryk, P. (2022). "Mapping Growth of the Russian Domestic Propaganda Apparatus on Telegram." *Challenges to national defence in contemporary geopolitical situations,* 2022(1), pp. 227–231.

53. Vernadsky, G. (1927). *Outline of Russian History*. Eurasian Publishing House.

54. Williams, E. M., and Carley, K. M. (2023). "Search engine manipulation to spread pro-Kremlin propaganda." *Harvard Kennedy School (HKS) Misinformation Review, 4(1)*, pp. 1-13.

55. Zeyliger, V. (2025). "The geopolitical conception of Russia's war on Ukraine: Neo-Eurasianism and Eurasian regionalism." *New Perspectives*, pp. 1-21.

56. Independent Institute of Socio-Economic and Political Studies. (2015). *The Most Important Results of The Public Opinion Poll In June 2015*. IISEPS. http://www.iiseps.org/?p=2678&lang=en.

57. Norris, R., and Merloe, P. (2015). Monitoring of Russian TV channels | 2015. Final Report. EaP Civil Society Forum Secretariat. https:// memo98.sk/ uploads/content_galleries/source/memo/russia/full-report-in-english. Pdf.

58. National Democratic Institute. (2016). Results of an April 2015 survey carried out for NDI by CRRC Georgia. NDI by CRRC Georgia. https://www.ndi.org/sites/default/files/NDI_November%202016%20poll_Issues_ENG_vf.pdf.

PRACTITIONERS' BROAD VIEW

SELFIE.ORG – SELF INTEREST EVALUATION OF FOREIGN INTELLIGENCE ENTITIES FOR ORGANIZATIONS

Florin BUŞTIUC*
Daniel DINU*

Abstract:
The pro-security attitude is necessary in an organization, for its survival from an economic and functional-administrative point of view. Therefore, an assessment of the existence of some situations may indicate an interest – incipient or developed – from some adverse/foreign intelligence entities, an assessment that subsequently determines the implementation and activation of some mechanisms for protecting values, such as personnel, facilities, information, equipment, networks and systems. As a principle, it is necessary for the organization to carry out a general verification of vulnerabilities, risks and threats through its own security structure, respectively through cooperation with state institutions.

Keywords: *economic espionage methods; sensitive information; security indicators; insider threat.*

Introduction

The state and private adversary intelligence structures target the institutions/organizations where information of interest of a political-diplomatic, military, social, administrative-legislative and economic nature is concentrated (and where strategies and decisions related to these areas are configured). If an adversary entity collects non-public information from the economic domain[1] (industrial espionage/

* Independent researcher, florinnn11@yahoo.com.
* Fellow at EuroMed Academy, daniel.dinu90@gmail.com.

[1] Sensitive information: *personally identifiable information* (personal details, identification numbers, digital identities, biometric records, personal characteristics or preferences); *financial information* (banking information, credit and debit card information,

corporate espionage, economic espionage), the following negative effects[2] may occur:

- *financial deficit* – compromising economic data correlates in most cases with significant financial losses (reputational damage and legal problems can also erode market shares and reduce profits).
- *loss of competitive advantage* – an adversary's access to non-public information can be transformed into the development of similar products or strategies.
- *reputational damage* – a successful attack by an adversary can erode the trust of customers and potential partners, investors.
- *legal implications* – in some cases, lawsuits may arise from investors or partners, who have also suffered from the espionage attack on your organization.
- *national security risks* – in some cases, the theft of information related to defence technologies or government projects could represent a threat to national security.

Information security, but also of other values – equipment, technologies, plans/strategies/decisions, people, etc. – is a necessity for the survival of an organization. Given that some of these values are also essential elements for national security, it follows that security becomes a necessary element at the organizational (private) and institutional (state) levels.

The general methods (*Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*) in which economic information is collected are the following:

1. *requesting information through e-mail or letters* – most requests are indirect, with reference to data available on websites, in advertisements, in articles in trade magazines and

transaction details, income and tax information, investment information); *health information* (medical history, diagnostic information, treatment records, health insurance data, family health history, lifestyle information); *business-sensitive information* (trade secrets, client information, employee information, strategic plans and research, contracts and legal documents, financial records, intellectual property); *high-risk data* (national identification numbers, biometric data, legal information, sensitive government information, sensitive corporate information), accessible to https://www.sealpath.com /blog/types-of-sensitive-information-guide/

[2] See more on https://www.ekransystem.com/en/blog/prevent-industrial-espionage

in marketing materials. Data collection (and as documentation for subsequent information requests) refers to publications and annual reports, patents, websites, marketing materials, conferences and exhibitions, professional contacts through membership in various associations – because there may be (inadvertently) sensitive/restricted information that becomes a support for directing the efforts to identify the connections of government entities with specific technologies and activities (AGGROS-aggressive open-source collection). Adverse information requests[3] are characterized as: a) initially legitimate questions that deviate into questions that clearly target sensitive, classified information, b) initially "banal" requests for price lists, catalogues, published works, research assistance, job counselling that become suspicious when they are characterized by insistence, persistence and focus on details, come from embargoed states, induce the idea of avoiding security and export control procedures.

2. *exploiting internet discussion groups* – the anonymity of the Internet is used in email-based discussion groups on various topics of interest related to recommendations for research activities and specific technical challenges (which may involve sensitive information and dual-use technologies).
3. *exploiting multinational conferences, business information exchanges or joint ventures* – such contexts represent an excellent pretext for gathering information (directly or through follow-up contacts) and for identifying and evaluating experts (in some cases, with specific cultural, ethnic, etc. backgrounds) in a particular field of interest.
4. *misleading open-source collection* – real interest, affiliation or location is camouflaged through "false associations" that create legitimacy/credibility of relationships, requests and reduce the likelihood of being identified as suspicious and reported/ ignored: use of the Internet from public libraries and educational institutions; routing e-mail through one or more countries to

[3] Adverse information requests – requests that, under the appearance of the normality of a relationship involving technical and psychological methods, ultimately aim to collect data of interest (sensitive, classified data).

hide the area of origin; use of contacts established within professional organizations and conferences.

5. *acquisition of export-controlled technologies* – the illegal acquisition of these types of technologies is carried out through: the use of front companies, transportation to an undeclared end user with forged certificates, the acquisition of an exportable version of a product and subsequent modification in the manufacturing process.
6. *theft of trade secrets, critical technologies, and critical information* – is carried out through classical intelligence services, state-sponsored educational and scientific institutions, private entities. But the current higher level of economic/ industrial espionage activities does not imply the disappearance of classical clandestine espionage – abroad, business people are potential targets, respectively, excessive elicitation is carried out at border crossings, hotel rooms are "searched", briefcases and laptops are "controlled".
7. *agent recruitment, co-optees and volunteers* – some people involuntarily become facilitators by arranging visits by foreign citizens to circumvent official procedures, present papers abroad, etc., and others voluntarily become agents[4].

Currently, courses are publicly provided on the use of HUMINT, including with reference to files and psychological profiles of potential sources; elicitation techniques; debriefing methodologies; information exploitation methods carried out at conferences and meetings. As a rule, human targets are[5]:

- *developers:* scientists, researchers, engineers who research and apply new materials/processes;

[4]Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, https://irp.fas.org/ops/ci/docs/fecie_fy00.pdf; and https://apps.dtic.mil/sti/tr/pdf/ADA465107.pdf; and https://www.travelsecurity.ch/Annual_Report_to_Congress_on_Foreign_Economic_Collection_and_Industrial_Espionage.html. See details on https://www.jlab.org/intralab/security/EconomicEspionageFactSheet.pdf and https://www.dcsa.mil/Portals/128/Documents/CI/DCSA_CI_Best_Practices_booklet.pdf*

[5] See more on https://www.dcsa.mil/Portals/128/Documents/CI/DCSA_CI_Best_Practices_booklet.pdf

- *technicians:* engineers or specialists who operate, test, maintain, repair technical systems;
- *production personnel*: personnel on production lines or in the supply chain area;
- *IT personnel:* system administrators, people with access to networks and knowledge of security protocols;
- *business development personnel:* marketing and sales representatives;
- *human resources personnel:* people with access to personnel and applicant records;
- *facility employees:* personnel who have access to spaces/ locations where information of interest is circulated, such as security personnel, cleaning personnel, etc.

The specific methods by which economic information is collected are as follows[6]:

1. *theft*: the theft of information or products;
2. *blackmail:* the use of threat or intimidation to provide information;
3. *mole planting:* the placement of a double agent in a competing company;
4. *eavesdropping/corporate communication intercepts*: ranges from telephone interception to the interception of Wi-Fi signals and emails;
5. *seduction:* a timeless technique that uses emotional elements to obtain information*;*
6. *bribery:* influencing an individual by offering money for information or to carry out illegal actions;

[6] Learning from the Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, *https://www.travel-security.ch/Annual_Report_to_Congress_on_Foreign_Economic_Collection_and_Industrial _Espionage.html. See details on DHS&CISA* - Chemical Security Summit *(2022), https://www.cisa.gov/sites/default/files/2022-12/summit-2022-intellectual-property-508.pdf and* Păstrarea unui secret comercial – Partea II [Keeping a Trade Secret – Part II], *https://ccir.ro/wp-content/uploads/2014/11/P%C4%83strarea-unui-secret-commercial-I.pdß*

7. *foreign intelligence recruits:* some private entities recruit former intelligence officers to carry out data collection activities of interest*;*
8. *hiring competitors' employees*: valuable employees are hired;
9. *bogus job interviews:* conducting fake interviews with candidates solely to gather key information about the employer and activities*;*
10. *social intelligence relationships*: developing "friendships" with various employees at professional meetings; dialogues with salespeople, distributors, loading and transporting personnel, former associates; eliciting former schoolmates, knowledge from various professional associations;
11. *bogus purchase negotiations:* some entities present themselves as "buyers" to obtain key information;
12. *research under false pretences:* the "author" uses the research paper to obtain key information;
13. *trade fair conversations:* establishing contacts at fairs, especially with experts. It correlates with capitalizing on: a) the tendency to provide excessive technical data/details during a conference presentation or during business meetings or negotiations with potential partners, suppliers, contractors, licensees, customers, b) project proposals or proposals that may contain sensitive, valuable information;
14. *dumpster diving:* searching for materials thrown in the trash;
15. *naturalized citizens:* requests addressed to naturalized citizens to provide information for patriotic or loyalty reasons (or threatening family members in the state);
16. *repatriating naturalized citizens:* attracting said persons to the state of origin to take over processes and methods;
17. *government debriefing:* interviewing one's own citizens upon their return from a foreign state to obtain information*;*
18. *outsourcing/offshoring:* outsourcing activities to foreign entities/offshoring can affect data security (for example, in some countries copyright laws do not apply);
19. *front companies and organizations:* foreign competitors pose as software vendors or even non-profit organizations in order to access trade secrets;

20. *joint venture & bidding process:* foreign buyers may require the provision of a large amount of data in the bidding process*;*
21. *"close proximity":* strategic partnerships and alliances create the opportunity for their own personnel to be exploited for information;
22. *mergers & acquisitions:* through these processes, technologies, innovations, etc. are acquired;
23. *front companies* (import-export front): the illegal export of documents, data or other sensitive items is carried out;
24. *altered products or false certifications:* companies from one's own state are exploited as intermediaries for the export of controlled products to a hidden end user through falsification of documents;
25. *university research:* private/state intelligence structures place agents in university research units;
26. *"excessive" negotiation:* excessive requests for information are made during negotiations;
27. *third-party acquisition:* the final recipients are individuals, companies or states that can obtain technologies, equipment, etc. only through such diversion*;*
28. *luggage or laptop theft:* luggage/electronic equipment from hotel rooms is "searched/taken" (in some cases, customs representatives "seize" laptops, tablets or mobile phones to copy data);
29. *Cyber Espionage methods:* exploiting website/browser vulnerabilities; attacking the supply chain, directly on primary partners or indirectly through Joint Venture; infecting third-party software application updates; distributing digital monitors accessible via wireless/external ports; requesting sensitive information through social engineering, phishing, compromising business emails, etc. (by choosing targets from lower/middle-level personnel, who are less likely to be suspicious).

In the context of presenting the general and specific methods of gathering information (from the economic area), we consider it appropriate to also present separately the internal organizational threat – the insider,

who is the person who has or has legitimate access to or knows the resources, including personnel, facilities, information, equipment, networks and systems.

The insider is represented by the current employee, contractual partners, temporary personnel engaged in the activities of the organization (out-sourcing contracts, internships, experience exchange, etc.), former employee, as follows[7]:

- a person in whom the organization trusts, including employees, members of the organization and those to whom the organization has provided sensitive information and access;
- a person who has received a badge or access device, which identifies him as a person with regular or continuous access (for example, an employee or member of an organization, contractor, salesperson, caretaker, repairman);
- a person to whom the organization has provided a computer and/or network access;
- a person who develops the organization's products and services, including those who know the secrets of the products that give value to the organization;
- a person who knows the fundamentals of the organization, including prices, costs and its strengths and weaknesses;
- a person who has knowledge of the organization's strategy and business objectives and is entrusted with future plans and the means to support the organization and to ensure the well-being of its employees;
- in the context of government functions, we have people with access to protected information, which, if compromised, could cause harm to national security and public order (*Insider Threat Mitigation Guide,* 2020, p. 9.).

The directions of action of the insider are represented by espionage, sabotage (physical or electronic), unintentional disclosure of information (to a third party or the media), facilitating access by a third party to the values of an organization (locations, information, personnel),

[7] Processed version of some aspects of the material *The human factor as a threat from within. Insider – understanding and approaches* (2023), related to the research activity within ANIMV.

theft of intellectual property, fraud by corrupting processes (altering internal processes, procedures and systems for financial or other purposes) (*Insider Threat Detection Study, 2018*).

Security indicators

The idea that, from an economic point of view, threats manifest themselves at the state and private level (but with effects in terms of national security) also correlates with the dimension of identifying a potential interest/ information gathering activity on the part of an adverse entity, a dimension that is circumscribed by security indicators.

Security indicators refer to observable behaviours, situations or circumstances that reveal that potential espionage or terrorist activities are being carried out, or other activities of gathering, transmitting, using, or disclosing unauthorized information. Reported to the insider, from the material *Analytic Approaches to Detect Insider Threats* (2015, pp. 14-24), two general types of indicators result, provided by *technical components* (systems/ computer programs, surveillance mechanisms and databases) and *non-technical* (data from security forms, self-declarations, personnel files, reports from colleagues and professional management).

Technical indicators (associated with the IT and physical surveillance system) (*Analytic Approaches to Detect Insider Threats*, 2015, pp. 14-24**):**

a. **authentication and authorization.** It is performed to access relevant resources of the organization, especially those considered fundamental to the organization's activity. These resources include data, services and capabilities and are available in operational systems, but also in backup systems. Failure to authenticate or attempted unauthorized access indicates an interest in data that is not related to professional duties.
b. **data access pattern** (specific time and frequency of access to relevant data). Changes in the access pattern indicate an interest in resources that were not previously associated with professional needs, potentially for unauthorized purposes. Access inconsistent with the user's class/level, related to

information that is not usually accessed in professional activity, may signal unethical purposes.

c. **network access/usage patterns** (specific protocols, source and destination, data packet sizes and frequency of sessions associated with user applications/operations). Changes in patterns (deviations from usual behaviour) signal changes in the user's goals, attitude and skills. It is a primary indicator for financial fraud and conjunctive data theft. Patterns inconsistent with the user's class/level (deviations from usual network traffic) may indicate possible disinterest or abusive behaviour. It is a primary indicator for accidental leaks, espionage and conjunctive data theft.
d. **data exfiltration** (unexpected or unauthorized movement of sensitive data from the organization's systems). A large/ unusual volume or certain types of data that "leave" the institution through printing services, e-mail or memory media is detected.
e. **unauthorized data access methods** (unauthorized or unusual connections to facilitate access or movement of data from the institution's official systems). Unauthorized connections of devices or between systems or unauthorized activities related to the movement/transmission of data are identified.
f. **system state changes with errors.** These are rapid changes in the system configuration that result in a state of insecurity, followed by attempts to repair the system to the initial configuration/state. It reveals inadequate training or system testing (unusually rapid changes in commands or a defensive posture associated with user errors and attempts to resolve these errors) and is a primary indicator for misuse and conjunctive data theft, and a correlation indicator for accidental data leaks and product alteration attacks.
g. **(inappropriate) use of commands**. Repeated occurrences of unexpected or unusual commands, related to the activity of colleagues, indicate a lack of training or testing of the system's response. It can be a correlation indicator for detecting accidental data leaks.

h. **access knowledge.** Efforts to acquire excessive knowledge, in contradiction with professional duties, may indicate "negative" goals of the user. Changes in data search patterns, including massive searches and directory browsing or access to a wide range of data, especially those not related to professional activity, are primary indicators for espionage, abuse and contextual data theft, and correlation indicators for financial fraud.
i. **change in audit logins.** The modification or deletion of security data or audit logins is detected.
j. **changes in pattern of access time**. Unexplained or unusual changes in a user's work schedule (logging into internal resources without credentials or multiple days of continuous access) could indicate an attempt to perform an activity while avoiding observation by colleagues or managers/ administrators.
k. **changes in pattern of access location**. Unexplained or unusual changes in the location(s) from which a user typically accesses a system indicate attempts to circumvent audit or security mechanisms, or to avoid observation by colleagues or managers/administrators.
l. **defect/error detection** (product defects or creation of unauthorized functionality). A pattern or history of product defects that do not correspond to the user's skill level may indicate negligence or an attempt to diminish or damage an organization's reputation, or to facilitate attacks against the organization's customer base. It is a primary indicator for sabotage attacks and could be a correlator for system misuse or workplace violence.
m. **malware execution**. Unauthorized installation/execution of an unauthorized program is an indicator for espionage, system misuse or sabotage.
n. **removal or modification of data or infrastructure**. Unauthorized deletion or change of data indicates behaviour that is likely intended to cause harm. It is a primary indicator for financial fraud, system misuse and product tampering.

o. **recovery (acts of unusual data recovery).** Recovering corrupted or deleted data from backup or archive indicates that data has been inadvertently deleted, or that there is an attempt to cover up traces of temporary changes or deletions. It is an indicator for conjunctive data theft and a correlator for accidental data leaks, financial fraud and system misuse.

p. **security breaches.** These are unauthorized activities that impact the security of an organization. Change in breach patterns - changes in the frequency or severity of security breaches are detected. Duration and regularity - monitoring incidents over time. Unauthorized or inappropriate use of tools, such as network analytics tools, that are specifically detrimental to the business/institution (installation of unauthorized functionality).

Non-technical indicators (personal, social and professional):

a. **competitor analysis**. It analyses capabilities or products that seem to indicate an advantage derived from knowledge of data that has not been made public. It identifies unexpected developments correlated with potential losses related to intellectual property. It is a primary indicator for espionage and system misuse.

b. **media analysis.** It identifies that unauthorized data has been disclosed. It is a primary indicator for espionage, system misuse or physical theft, and it is an indicator of correlation of accidental data leaks.

c. **recent increase in criminal activities.** Criminal activity can damage the reputation of an organization or pose a threat to the organization or its employees.

d. **violence outside the workplace.** Stress and violent behaviour outside the workplace can indicate an increased likelihood of violence against the organization or colleagues.

e. **major life events**. Major life events (e.g., change in marital status, birth of a child, or death of a relative) can impact work behaviours and create tensions that precipitate inappropriate decisions.

f. **changes in financial and material possibilities** (unexpected resources or debts). *Observable changes over time* – a sudden influx could indicate that an individual is being bribed or influenced to carry out a harmful activity; sudden and excessive debts may be associated with stress that can impair rational capacity. *Changes in comparison with colleagues* – differences can create tensions that impact decision-making. *Financial reports* – significant changes reported by financial reports or other external sources may indicate hidden wealth or financial stress.
g. **salary withholdings**. Legal actions to collect debts indicate financial stress that may warrant additional scrutiny of an individual related to financial fraud attacks.
h. **unusual contacts** (contacts with individuals or groups carrying out potentially negative/harmful activities, which may indicate that those relationships have an inappropriate influence on the employee). *Unusual business trave*l – changes in business travel to foreign countries not usually visited in the normal course of business, or meetings with representatives of these countries. *Personal travel* – discovery of frequent travel to foreign countries not usually visited in the normal course of business, or meetings with representatives of these countries (this is noted if the employee has attempted to conceal the travel). *Unauthorized or inappropriate associations* with hostile groups or participation in their actions may indicate a change in loyalty/belief/mentality, which may precede acts of deterioration of an organization's values.

We supplement the security indicators related to insider (which focus on the internal perspective of the threat) with indicators[8] that

[8] Indicators processed from the *Mini-guide for Counter-Information Training and Protection* (2015, Bușticu Florin), Bucharest, SemnE Publishing House, and capitalizes on the following materials: *Department of the Army*. (1993). *Army Regulation 381–12. Military Intelligence Subversion and Espionage Directed Against the U.S. Army (SAEDA) and* Counterintelligence Office of the Defence Investigative Service. (2000). *Suspicious indicators and security countermeasures for foreign activities directed against the US Defence Industry*, https://irp.fas.org/doddir/army/ar381-12-1993.pdf; Department of Commerce - Office of Security. (2006). *Suspicious Indicators and Security Countermeasures*

highlight the *relational dynamics of insider-suspicious activities of a foreign entity*.

Indicators that the organization's personnel are in the attention of an adverse information structure (Buştiuc, 2015):

a. some employees receive (unusual) congratulations or other correspondence from the embassy of the country of origin;
b. some employees receive invitations to visit the country of origin, to give a scientific presentation or to receive an award;
c. foreign visitors try to selectively relate to personnel who show similarities (cultural, ethnic, religious, etc.);
d. some employees from sensitive sectors of the organization are insistently and frequently sought out by former colleagues.

Indicators that the organization is the subject of intelligence gathering activities (Buştiuc, 2015):

*a. application for employment***:** some individuals offer their services under minimal financial conditions, stating that a foreign state/company bears the costs; the field in which the person chooses to work is related to a military component or involves classified technology.
b. assistance/partnership activities: provision of software products and assistance from "offshore" states; offering government or "business" scholarships; invitations for intercultural exchanges, through individual partnerships or within a general program.
c. co-opting of former employees: a former employee is employed by a company with the same field of activity; the former employee actively maintains contacts with some members of the organization.
d. activities within contract negotiations: unjustified requests for access to the internal computer network; requests for unrestricted physical access; requests to transmit a large volume of technical data in order to subsequently cancel the contract; sending a disproportionate number of representatives.

---

for Foreign Collection Activities Directed against the United States, https://apps.dtic.mil/sti/tr/pdf/ADA470350.pdf; Defence Security Service. *Counterintelligence CI Best Practices for Cleared Industry*, https://security.research.ucf. edu/Documents/CI/Counterintelligence%20Best%20Practice%20for%20Industry.pdf

e. *foreign visits:* people added to the visitor list at the last minute; visitors ask questions that go beyond the topics set for discussion (they rely on polite answers); visitors ask for a lot of data and in return provide general explanations; some visitors do not have the necessary experience/qualification in the field; "lost" visitors, who appear offended when explanations are asked about their presence in a space other than the designated one; a visitor who is very curious about employees, programs and work areas that were not included in the agenda.
f. *exhibitions, seminars:* the topics are related to classified topics; the state or organization sponsoring the seminar previously requested visiting some objectives but a refusal was made; invitations to present a specific topic, which include all costs paid; requesting a summary of the paper 6-12 months in advance and requesting development/detailing of some aspects; conversations during and after these events in which other professional aspects are attempted to be addressed.
g. *actions of personnel exploitation*: technical means of surveillance are introduced in hotel rooms, meeting spaces; attempts are made to create compromising situations; excessive requests for assistance and advice.

Information, technology, people, reporting/signalling methods are the fundamental elements for a threat identification and mitigate program – each element can independently provide a suspicious aspect, but the correlation/integration of the elements reveals the significant aspect indicating the existence of an internal and/or external threat. In this context, we consider the SELFIE.org questionnaire useful as a tool for organizational self-assessment of the interest of adversary/ foreign entities.

There are 45 questions that refer to situations that signal a potential informational interest of an adverse entity (natural person & legal entity, state) – organization, institution, competitor/adversary state or potential partner, adverse state intelligence service, adverse private intelligence structure (and their representatives). The questionnaire is intended to be completed by decision-makers – since an attempt was

made for the questions to cover situations valid simultaneously for state and private organizations, regardless of the situation, it is mandatory to select an answer related to the viability of the situation for one's own organization (even in particular/ atypical cases).

Annex 1: The SELFIE.org questionnaire

1. Do employees frequently report that there are adverse entities that are interested in obtaining classified/non-public information?
□Yes □No
2. Do employees frequently report that at various conferences/meetings, topics are addressed that demonstrate knowledge of data that has not been made public?
□Yes □No
3. Do employees report that during meetings/conferences they are asked "innocent/camouflaged" questions in order to collect sensitive information?
□Yes □No
4. Are there any signs that some of the competitors are aware of negotiation strategies/objectives?
□Yes □No
5. Does non-public information about your organization appear in the media or specialized publications?
□Yes □No
6. Does an adversary entity eliminate you from different markets, fields, partnerships, negotiations, etc. with similar products and services?
□Yes □No
7. Do adversary/foreign entities carry out recruitment procedures for their own experts by conducting "interviews" for a possible employment, in which explanations, details related to sensitive data are atypically requested?
□Yes □No
8. Do employees report that they have been asked by adversary/foreign entities to carry out "extra-professional" studies, syntheses, translations, etc. related to sensitive data?
□Yes □No
9. Do laptops, documents, USBs containing important information disappear in uncertain situations?
□Yes □No

10. Before/during the steps associated with the act of resignation, does one or more employees avoid, do not make concrete references to the new job?
□Yes □No
11. Are there constant, unusual requests for planning visits to the organization's headquarters or different branches?
□Yes □No
12. Are there unannounced requests for information (in the form of questionnaires, market studies, etc.) by e-mail/telephone and are they addressed in most cases to people who are not part of the responsible specialized department (public relations etc.)?
□Yes □No
13. Are topics addressed that were not included in the discussion program, is the list of visitors changed at the last minute, are visitors accompanied by embassy officials who try to protect their identity and minimize the expression of an official position?
□Yes □No
14. Does an adversary issue invitation to attend international seminars, meetings, after failing to plan a visit to your organization's headquarters?
□Yes □No
15. At (international) seminars/meetings, do some participants carry incomplete or false identification marks?
□Yes □No
16. Do foreign visitors select staff who have a similar cultural/ethnic background, in order to network, socialize or carry out a joint professional activity?
□Yes □No
17. In the context of official visits, do some visitors seem to not have the same level of expertise as others, are they not attentive/not focused on the agenda of the visit?
□Yes □No
18. In the context of official visits, does a "lost/confused" visitor feel offended when asked for explanations regarding his presence in a space other than the one designated for visitors?
□Yes □No
19. During trips abroad, are attempts made to create compromising situations (staging a theft, an accident, drug possession, a situation of infidelity etc.)?
□Yes □No

20. Have been received emails requesting information about your organization or an employee's professional activity?
□Yes □No
21. During the hiring process, do some individuals offer their services at minimal financial terms, stating that a foreign state/organization is covering the costs?
□Yes □No
22. During the hiring process, is the field in which the individual chooses to work related to a military component, dual-use or export-restricted technology, or classified topics?
□Yes □No
23. During assistance/partnership activities, are products and software support provided from "offshore" states?
□Yes □No
24. During assistance/partnership activities, are government or "business" scholarships offered?
□Yes □No
25. During assistance/partnership activities, are invitations made for intercultural exchanges, through individual partnerships or as part of a general program?
□Yes □No
26. Are several former employees employed by an organization with similar fields of activity?
□Yes □No
27. Do a former employee(s) actively maintain contacts with some members of the organization?
□Yes □No
28. During negotiation activities/professional exchanges, are there unjustified requests for access to the internal computer network?
□Yes □No
29. During negotiation activities/professional exchanges, are there requests for unrestricted physical access?
□Yes □No
30. During negotiation activities/professional exchanges, are there requests to transmit a large volume of data in order to subsequently cancel the conclusion of the contract?
□Yes □No

31. During negotiation activities/professional exchanges, are there a disproportionate number of representatives from an adverse entity sent?
□Yes □No
32. During visits by foreign delegations, are there people added to the visitor list at the last minute?
□Yes □No
33. During visits by foreign delegations, do visitors appear who ask questions that go beyond the topics set for discussion?
□Yes □No
34. During visits by foreign delegations, do visitors appear who request a lot of data and instead provide general explanations?
□Yes □No
35. During visits by foreign delegations, a visitor who is very curious about employees, programs and work areas that were not included on the agenda?
□Yes □No
36. During visits by foreign delegations, is assistance and advice excessively requested?
□Yes □No
37. Are the topics proposed/addressed during exhibitions, seminars, meetings related to sensitive, classified topics?
□Yes □No
38. An adversary entity that was denied meetings, visits to objectives, transmission of certain data, etc., subsequently sends invitations to exhibitions, seminars that it organizes/sponsors?
□Yes □No
39. Does an adversary entity send invitations to exhibitions, seminars, etc. where it pays all the costs paid, but with the express request to present certain topics?
□Yes □No
40. When organizing exhibitions, seminars, is a summary of the material previously requested and then, in a phased manner, the development/ detailing of certain aspects?
□Yes □No

41. When organizing exhibitions, seminars, do conversations occur during and after these events in which other professional aspects are attempted to be addressed?
□Yes □No
42. During trips abroad, do employees report that they had the feeling that they were being watched/there were technical means of surveillance in hotel rooms, meeting spaces?
□Yes □No
43. Is employee/some employees involved in unauthorized Internet discussion groups where various topics of interest related to professional activity are addressed?
□Yes □No
44. Has employee/employees been requested information about colleagues, professional activity, etc. by foreign authorities at border crossings or in the context of incidents on the territory of the respective foreign state?
□Yes □No
45. Does employee/employees perform (massive) data searches and consult directories that are not correlated with professional activity?
□Yes □No

How to interpret the scores (the sum of the Yes answers):
1-15 – normally, an organization is a target for an adversary/competing entity, and the score highlights that you are within the normal limits of a "probing". The recommendation is to implement or specifically activate a mechanism for awareness and reporting by all employees of security indicators, respectively physical and IT mechanisms for identifying intentions to access unauthorized spaces, equipment and data.
16-30 – is a signal that there is an active, sustained interest from an adversary entity. The recommendation is to ask the security structure to re-evaluate the effectiveness of security policies and rules, physical and IT protection mechanisms, to apply security questionnaires to assess the level of knowledge and training of personnel, respectively to conduct training sessions in different specific areas. It is also necessary for the security structure to carry out various exercises to test the application of the rules and the functioning of the mechanisms, respectively to ensure

that the signalling of security indicators is working. At the level of decision-makers, it is necessary to define the appropriate responses/ reactions at the administrative and legal level to eliminate vulnerabilities and risks.

31-45 – it is necessary for the organization to carry out a general verification of vulnerabilities, risks and threats (compliance with security rules, IT access, personnel re-evaluations, and interviews with personnel, etc.) through its own security structure, respectively through cooperation with state institutions.

References:

1. Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*. https://irp.fas.org/ops/ci/docs/fecie_fy00.pdf and* https://www.travel-security.ch/Annual_Report_to_Congress_on_Foreign_ Economic_ Collection_and_Industrial_Espionage.html

2. *Buştiuc, Florin. (2015).* Mini-guide for Counter-Information Training and Protection*, Bucharest, SemnE Publishing House.*

3. *Buştiuc, Florin. (2023).* The human factor as a threat from within. Insider – understanding and approaches*.*

4. *Cybersecurity and Infrastructure Security Agency. (2020)*. Insider Threat Mitigation Guide, *p. 36, https://www.cisa.gov/sitesdefault/files/publications/ Insider%20Threat%20Mitigation%20Guide_Final_508.pdf*

5. *Defence Security Service. (n.d.).* Counterintelligence CI Best Practices for Cleared Industry.*https://security.research.ucf.edu/Documents/ CI/Counterintelligence%20Best%20Practice%20for%20Industry.pdf*

6. *DHS&CISA* – Chemical Security Summit*. (2022). https://www.cisa.gov/ sites/default/files/2022-12/summit-2022-intellectual-property-508.pdß*

7. *Department of the Army. (1993).* Army Regulation 381–12. Military Intelligence Subversion and Espionage Directed Against the U.S. Army (SAEDA). *Counterintelligence Office of the Defence Investigative Service. (2000).* Suspicious indicators and security countermeasures for foreign activities directed against the US Defence Industry, *https://irp.fas.org/doddir/army/ar381-12-1993.pdf*

8. *Department of Commerce – Office of Security. (2006).* Suspicious Indicators and Security Countermeasures for Foreign Collection Activities Directed against the United States*, https://apps.dtic.mil/sti/tr/pdf/ADA470350.pdf*

9. Insider Threat Detection Study. *(2018). NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf*

10. Learning from the Annual Report to Congress on Foreign Economic Collection and Industrial Espionage. *https://www.travel-security.ch/Annual_Report_to_Congress_on_Foreign_Economic_Collection_and_Industrial_Espionage.html*

11. Păstrarea unui secret comercial – Partea II [Keeping a Trade Secret – Part II], *https://ccir.ro/wp-content/uploads/2014/11/ P%C4%83strarea-unui-secret-commercial-I.pdß*

12. Software Engineering Institute. (2015). *Analytic Approaches to Detect Insider Threats,* pp. 14-24. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=451065

INTELLIGENCE AND AI

Eros-Adrian ASĂNACHE*

Abstract:
In today's reality, marked by technological transformations at an accelerated pace, Artificial Intelligence (AI) is emerging as a new player in intelligence operations, thus redefining the traditional paradigms of intelligence collection, analysis and exploitation. This paper aims to analyse the practical applications of AI, the challenges and benefits brought to Intelligence work. In the same context, it should be mentioned that the ethical and strategic risks generated by the integration of AI in the decision-making process will also be discussed, ranging from simple algorithmic errors and unintentional discrimination to the threat posed by deep fake information manipulation. Thus, a balanced approach is required between technological innovation and the benefits of AI, and the responsibility of the measures taken, by generating a modern intelligence system that meets both the security needs of states and their democratic values.

Keywords*: artificial intelligence; intelligence operations; national security; digital surveillance; deep fake.*

Introduction

The accelerated technological developments of the 21st century have led to profound transformations in national security. In a global context where hybrid threats, transnational terrorism, cyber warfare and international conflicts are present, the way of looking at the conduct of intelligence operations needs to be rapidly adapted by national security agencies. Today's realities show that major world powers such as the US, China and EU states are adapting their intelligence structures to new digital realities.

* Graduate Student, "Mihai Viteazul" National Intelligence Academy, e-mail: erosadrianasanache@ gmail.com. Disclaimer: the material is a reflection of the authors' opinions and beliefs, and does not represent the opinions, policies or the views of the Romanian Intelligence Service or the National Intelligence Academy "Mihai Viteazul".

Artificial intelligence is gaining increasing importance in national security issues by offering extended capabilities to analyse, anticipate and respond to contemporary threats. AI is thus emerging as one of the most revolutionary tools in this respect, which can increase the efficiency of operations, while at the same time facing challenges related to their ethical and legal nature.

The aim of the paper is to highlight how AI has begun to transform the information activity by moving to a digitized system defined by automations, decision algorithms and predictive-predictive systems. The difficulties in this field are also represented by the delegation of decision to non-human systems, with the possibility of generating errors in strategic contexts and the impossibility to control the effects of such decisions. In this paper, analytical methods such as factorial and cost-benefit analysis will be addressed, based on information obtained from the online environment.

Technologies with practical application in intelligence work

Technologies refer to the totality of techniques, methods, processes and tools used to create goods or services or to achieve objectives.

Since 2020, with the onset of the COVID-19 pandemic, there has been an explosion in the volume of online data. Big Data thus began to take on increasing importance, with algorithms beginning to learn, analyse and turn data into forecasts. The years 2021 and 2022 see a massive development of machine learning related processes. Starting in 2023, Big Data is helping to create intuitive platforms and complex analytics at the click of a button, also at the same time concerns about GDPR compliance are growing. In 2025, Big Data can be defined as a true partner, where it is no longer just a tool, but a partner.

Machine Learning (ML): performs automated analysis of big data; moreover, ML can predict reactions and actions based on already learned patterns and generate relationships between actors and events. For example, ML algorithms are used in cyber-attack prevention systems to detect suspicious behaviours before they become real threats, such as the Darktrace platform, which uses ML for corporate network security (Sommer and Paxson, 2010).

Natural Language Processing (NLP): is used to analyse and extract the essential meaning of written or spoken texts, for example in the detection of hostile actions against national security of subversion, extremism or terrorism. An example is the use of NLP in online message monitoring to identify radical speech and terrorist plots, such as the Jigsaw Perspective platform used to detect hate speech on the internet (Burnap and Williams, 2015).

Computer Vision: takes place by analysing satellite or drone imagery; it uses facial recognition technology and has practical application in monitoring and identifying suspicious persons in public spaces. For example, surveillance systems in major cities such as London use facial recognition to detect suspects in crowds (*Jain et al., 2016*).

Anomaly Detection: detection of atypical or risky behaviour; practical applicability for intelligence agencies as it easily detects unusual activity that could signal an imminent threat. An example is the use of anomaly detection in network traffic monitoring to identify cyber-attacks, as in the solutions offered by the company Splunk (Chandola et al., 2009).

Practical applications of AI in Intelligence

Nowadays, AI can be used in intelligence operations to achieve results faster and with greater efficiency. Technological developments mean a new approach in this area too. Models for the use of AI in the intelligence area are generally represented by the automation of OSINT analysis processes, the detection of behavioural patterns of actors involved, video surveillance through facial recognition and countering cyber threats.

Automating OSINT analysis. With the ability to mass process data from social networks, forums, news feeds and other online platforms, AI can accomplish (Wasserman, and Faust, 1994). Rapid identification of relevant actors: whether we are talking about suspects, organized groups or organizations, AI can understand their dynamics and predict their future actions based on the relationships between actors. Network analysis helps to prevent illegal activities by monitoring the evolution of networks and intervening quickly at identified key points.

a. Detect signs of radicalization: certain sudden behavioural changes can be easily observed by AI, which is useful for identifying the person or group that may become a threat Procedural algorithm can recognize changes in real time based on content analysis.

b. Automated decision making: after collecting and analysing data, AI can contribute to its value by forwarding recommendations and actions to be taken, thus prioritizing areas of interest for state actors and security agencies. Big Data platforms could develop the ability to filter alerts based on severity and likelihood.

Combating cyber threats. AI helps to detect cyber-attacks in real time by scanning network traffic and reporting anomalies: "Machine learning techniques offer significant promise for real-time anomaly-based intrusion detection by identifying deviations from normal network traffic behaviour." (Sommer and Paxson, 2010, p. 306) Machine learning algorithms have the ability to identify new types of cyber-attacks that traditional systems would not have detected. Unlike traditional intrusion detection systems (IDSs), which rely on fixed signatures of known attacks, machine learning (ML) algorithms have the ability to also identify new or unknown cyber-attacks.

AI is proving to be essential in this regard as it enables not only continuous network monitoring, but also automatic reaction to emerging threats, even previously unknown attacks (Buczak, and Guven, 2016). Thus, some examples are represented by:

a. Responding to attacks through autonomous defences: not only can AI detect attacks, but it also has the ability to autonomously respond to them; AI can block a suspicious IP, isolate a compromised area of the network, or temporarily disable sensitive processes to prevent serious consequences to the cyber architecture. A successful example is the Darktrace Antigena system, deployed in government and private sector organizations, which uses AI to understand the normal behaviour of IT infrastructure and intervene immediately when it detects deviations.

b. Predicting future attacks: access to databases containing past attacks, coupled with the ability to analyse long-term anomalous behaviours, AI can help intelligence agencies develop preventive strategies and predict the types of attacks that are likely to manifest in the coming period. One notable example is the use of AI at MIT Lincoln

Laboratory, where researchers developed a system that, based on network data collected in real time and a history of attacks, could predict with high accuracy spear-phishing attempts or lateral moves into infrastructure up to 48 hours before the actual impact.

Facial recognition and video surveillance. The use of facial recognition and video-surveillance, with the involvement of AI, is an essential solution in monitoring and identifying individuals in real time (Jain, Ross and Nandakumar, 2011, p. 98).

a. Large-scale surveillance: large cities have a multitude of surveillance cameras, and AI has the advantage of simultaneously analysing thousands of security cameras to identify individuals or groups of interest, independent of manual human analysis; this allows quick and efficient operational decisions to be made on the targets of security agencies. For example, in Chongqing (China) or London (UK), video surveillance networks in Chongqing (China) or London (UK) use facial recognition systems integrated with AI to locate wanted persons in real time without the need for continuous manual monitoring.

b. Improved accuracy: AI has the ability to adapt to changes in the environment and recognize people from a distance or in low-light, moving or static conditions, proving to be more effective than traditional systems. For example, the Clearview AI system, used by some US police forces, has demonstrated a high recognition rate even on distorted or low-quality images

c. Detection of suspicious activities: certain behaviours, actions or movements made by people in the environment can be easily identified by AI which, based on algorithms, sends signals to a human operator who can then take operational action against them. The Behavioural Recognition System developed by BriefCam and deployed in airports in Israel and the USA provides real-time alerts to human operators, who can intervene promptly to prevent incidents or attacks.

Drones and advanced robotics. Drones and robots represent another stage in the evolution of modern intelligence, with practical application in missions where human action would be impossible and risky, jeopardizing the entire operational success of a mission. Thus, of interest in this area would be:

a. Reconnaissance missions in inaccessible areas: UAVs with AI capabilities have the ability to penetrate conflict zones, radioactive environments or other hazardous areas, increasing the security of operations and reducing risks. For example, the **RQ-11 Raven** and **Black Hornet Nano** drones, used by the US military and NATO, have been deployed in combat zones such as Syria and Afghanistan to provide real-time tactical reconnaissance without exposing soldiers to danger.

b. Autonomous decision making: drones with AI capabilities can move and make decisions without human intervention, such as avoiding obstacles, adjusting the trajectory based on weather conditions or identifying a more efficient alternative route while allowing surveillance of the target. For example, **Skyborg** drones, developed by the U.S. Air Force, can operate semi-autonomously in reconnaissance and air support missions, using AI to make tactical decisions without constant human control.

c. Long-term monitoring and data collection: autonomous drones can carry out long-term monitoring missions, reducing reliance on human resources and maximizing efficiency, including in hard-to-access or dangerous areas. An example is the use of **Sentinel** drones by EU border agencies for continuous monitoring of external borders, including at night and in difficult weather conditions. This reduces costs and the reliance on permanent human patrols.

Challenges and risks

Ethical issues. In my opinion, the use of AI in intelligence entails major ethical risks. First, automating decisions could potentially lead to algorithm-based discrimination. Biased models may be brought into the data analysis, meaning that the judgment may not be correct. I believe that individual rights and freedoms may be affected by the lack of transparency in decision-making, so security agencies have an obligation to strike a balance between technological efficiency and the fundamental principles to be respected in the rule of law.

Technological vulnerabilities. In terms of deep fake and other forms of artificially generated content, there is a risk in allowing false information to be disseminated quickly and efficiently, but dangerously at the same time. These tools can be used in influence or disinformation

operations, putting a huge strain on information security. European intelligence services have warned that groups backed by hostile states are using AI-generated content to influence public opinion during election campaigns or social protests. Thus, my opinion is that it is becoming an imperative requirement for security agencies to develop robust cyber detection and defence capabilities, while maintaining control over the integrity of AI systems.

Over-dependence on technology. The embedding of AI capabilities in more and more intelligence operations (e.g. in automated information selection and sorting, analysis of behavioural patterns or generation of operational alerts) may create the conditions for a dependency on this technology.

In this context, I can note that there is a reduction in the processing, critical analysis and rapid reaction capacity of members of security agencies. I also consider that the adaptability of the human factor, often regarded in the intelligence area as its most important quality, is thus visibly vitiated by not training it in decision-making and adopting a predetermined one generated by AI.

In the same context, when the algorithms have not had proper training or the data has been inconsistent, the decisions that the AI generates may be inappropriate or noticeably erroneous. This phenomenon is commonly seen in AI systems that suffer from "data bias" or "biased training data," leading to skewed results. For example, in 2018, a criminal recidivism risk prediction system used in the US, called COMPAS, was criticized for overestimating the risk of recidivism in people of colour based on biased historical data, leading to controversial judicial decisions. The fact that AI systems could decide on their own the operational decisions to be taken could lead to huge strategic losses, which is why it is essential to keep the operational decision in the hands of the security agencies, with human factors driving it, human expertise proving to be essential in the analysis and decision process.

Conclusions

The integration of advanced technologies is a modern-day imperative for state security agencies to achieve. At the same time, the practical applications of AI in the field of intelligence operations, which

demonstrate its significant potential: from identifying cyber threats and monitoring online behaviour, to crisis management and critical infrastructure protection, are worth watching closely. These come with a range of risks and vulnerabilities, with ethical, legal and social challenges raising important questions about the application of automated operational decisions. The key to the sustainability of AI in national security is a balanced approach, where technological innovation and respect for fundamental human rights are intertwined. In conclusion, AI is not just a set of technological methods and means, but a strategic component that needs to be carefully integrated into the national security architecture and intelligence operations of the future.

References:

1. Buczak, A. L., and Guven, E. (2016). "A survey of data mining and machine learning methods for cyber security intrusion detection." *IEEE Communications Surveys & Tutorials*, 18(2), pp. 1153-1176.

2. Burnap, P., and Williams, M. L. (2015). "Cyber hate speech on Twitter: An application of machine classification and statistical modelling for policy and decision making." *Policy & Internet*, 7(2), pp. 223-242.

3. Chandola, V., Banerjee, A., and Kumar, V. (2009). "Anomaly detection: A survey." *ACM Computing Surveys (CSUR*), 41(3), p. 15.

4. Jain, A. K., Ross, A., and Nandakumar, K. (2011). *Introduction to biometrics*. Springer.

5. Jain, A., Ross, A., and Nandakumar, K. (2016). *Handbook of biometrics*. Springer.

6. Sommer, R., and Paxson, V. (2010). "Outside the closed world: On using machine learning for network intrusion detection." *2010 IEEE Symposium on Security and Privacy*, pp. 305-316.

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

8. Russell, S., and Norvig, P. (2020). *Artificial Intelligence: A Modern Approach* (4th Ed.). Pearson.

9. Goodfellow, I., Bengio, Y., and Courville, A. (2016). *Deep Learning*. MIT Press.

10. McKinsey Global Institute. (2018). *Notes from the AI frontier: Applications and value of deep learning*. McKinsey & Company.

11. Floridi, L., and Cowls, J. (2019). "A unified framework of five principles for AI in society." *Harvard Data Science Review*.

12. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., and Floridi, L. (2016). "The ethics of algorithms: Mapping the debate." *Big Data & Society*, 3(2).

13. Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.

14. Zeng, Y., Lu, E., and Huangfu, C. (2019). "Linking artificial intelligence principles." *Association for Computing Machinery*.

15. Choi, E., & Choi, S. (2019). "Advances in AI applications in cybersecurity." *IEEE Access*, 7, pp. 95343-95362.

16. Brundage, M., Avin, S., Clark, J., et al. (2020). *Toward trustworthy AI development: Mechanisms for supporting verifiable claims*.

17. Brown, T. B., Mann, B., Ryder, N., et al. (2020). "Language models are few-shot learners." *Advances in Neural Information Processing Systems*.

18. OpenAI. (2023). *GPT-4 Technical Report*. OpenAI.

19. Varshney, K. R. (2016). "Engineering safety in machine learning." in *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*.

20. Office of the Director of National Intelligence (ODNI). (2021). *Artificial Intelligence and National Security*. U.S. Government Report.

21. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2022). *Artificial Intelligence and Cyber Defence*.

22. US Department of Defence. (2019). *Summary of the 2018 Department of Defence Artificial Intelligence Strategy*.

23. European Commission. (2021). *Proposal for a Regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act)*.

24. Mozur, P. (2019). "Inside China's dystopian dreams: AI, shame and lots of cameras." *The New York Times*.

25. Liu, H., & Fan, W. (2020). "AI-enabled security technologies for the Internet of Things." *IEEE Internet of Things Journal*.

26. Nguyen, T. T., and Nguyen, Q. H. (2021). "Detecting deep fakes using neural networks: A survey." *IEEE Transactions on Information Forensics and Security*.

27. West, D. M. (2018). *The future of work: Robots, AI, and automation*. Brookings Institution Press.

28. Crootof, R. (2016). "The killer robots are here: Legal and policy implications." *Cardozo Law Review*, 38(5).

29. Bryson, J. J. (2018). "Patience is not a virtue: The design of intelligent systems and systems of ethics." *Ethics and Information Technology*, 20(1), 15-26.

GAMES, EXERCISES AND SIMULATIONS

MOOT COURT EXERCISE – CASE OF TREASON THAT MAY INVOLVE ONLINE FORUMS

Andrei-Alexandru STOICA*

Introduction

The present exercise aims to portray a situation regarding the publication of sensitive information on the internet. The exercise outlines how members of the armed forces post on different forums, in our case a gaming forum, sensitive data regarding military gear, and the scope is that state authorities have to establish whether said posts can be legally classified as treason, either generally or a special form of said crime.

Format, roles and assignment

The exercise will require at least five participants, that have studied and acquired basic knowledge of civil and criminal law, have a basic understanding of internet usage and culture and also have grasped notions regarding national security and its issues. Each participant will have a role to play in the exercise and each will have a different objective that must be attained, the final decision being open to interpretation based on the facts presented by the participants.

The participants will be able to have the following roles and aims:

1. Judge – who has to hear the parties, read and understand their claims and deliver a decision.

* Assistant PhD, "Mihai Viteazul" National Intelligence Academy, email: stoica.andrei@animv.eu. Disclaimer: the material is a reflection of the authors' opinions and beliefs, and does not represent the opinions, policies or the views of the Romanian Intelligence Service or the National Intelligence Academy "Mihai Viteazul".

2. Prosecutor – who has to draft the indictment and present the grounds for bringing the case to trial.

3. Legal counsellor of the military agency (the victim) – who has to outline the institution's situation, contextualize the issue and present its conclusions.

4. Legal representative of the accused - The accused and his legal representative have to present its defence and prove that the objective and subjective elements of the alleged offence have not been met.

5. The representative of the legal person owning the gaming website where the leaks happened – who must offer technical support and present its story as a platform owner. This last role has been considered to be played as an expert opinion or that of a witness.

The case is constructed as being a situation in which all participants are allowed to present their opinions, claims and conclusions, all in a simulated case based on a fictional scenario, but based on real issues that have transpired between July 2021 and June 2025. The participants must abide to the legal procedures in front of a court and must present their claims, opinions, facts and evidence according to legal norms. The case is a fictional one, but will be conducted base on Law no. 135/2010 regarding the Criminal Procedure Code of Romania, in its updated version.

Background

The case involves the situations that have been observed on the gaming website of the developer Gaijin Entertainment, known for the online free-to-play game *War Thunder*. The War Thunder forums have been known for the past few years as a place in which a lot of military documents have been posted by users who had access to these types of documents. A large part of the leaked documents are marked in such a way that they are not meant for public release and are restricted to authorized government personnel and contractors. The leaked documents have been noted to be from the United Kingdom, France, and People's Republic of China, the United States of America, the Russian Federation, Germany and Italy. While the information being mostly technical documents that comprise mechanical aspects of machines that are actively by the armies of different states, Gaijin Entertainment

took measures to ban users, albeit temporary, and to delete the sensitive information.

The participants to the simulation game must decide if the information in the exercise can be considered sensitive enough to be classified information or can be classified as an act of a lesser severity.

Structure of the case

The case will be structured as it follows, but may be modified to suit the needs of the exercise, context and the level of legal knowledge of the participants.

Directorate for Counter-Terrorism and Organized Crime, CASE NO. 999/P/2025, INDICTION

A. Information on the defendant: Andrei Popescu, born on 1st of April 2000, living in Bucharest, Romania, Minotaurului Street, working as a software engineer at Red Rings of Power Inc., no criminal history.

B. Context and facts of the case

During March and throughout April 2025, the defendant Andrei Popescu, a user on the forum hosted by Taijiro Gaming, posted the following materials:

1. Technical manual of the T-99 Panther tank, an armoured vehicle currently in service with the Romanian Army. The material was marked "Confidential – restricted distribution" and was posted in threads dedicated to discussions about military vehicle performance within the game;
2. Experimental manual of the Vortex aircraft, under testing, marked "Cosmic Top Secret", containing information on the prototype aircraft not intended for public release.

Taijiro Gaming offered an official explanation regarding these posts:

- The forum is a public, moderated space, where users discuse mil-sims;
- There have been similar leaked documents before, but moderators removed sensible content in a quick manner;

- The company claims that the posts were for entertainment purposes and to outline technical prowess;
- The forum fosters discussions among enthusiasts regarding mil-sims and real-world technology;
- Forum culture often promotes competitive sharing of unusual or technical knowledge, with users trying to impress others by revealing "hidden" data;
- Similar incidents have happened before, with users posting technical manuals or performance data for discussion. The company has a process to remove sensitive content, but the forum supports technical debate and sharing within a hobbyist context.

The cyber investigation showed that only a few users downloaded the documents, and there is no proof they got into the hands of foreign agencies. However, the prosecutor considers that these actions should be considered as grounds for treason, claiming that data about the T-99 Panther can be considered as state secret and that the Vortex manual is a classified document.

Andrei Popescu explained that his main reason for sharing the T-99 Panther manual was to boast within the online community. In gaming forums like Taijiro Gaming, users often display knowledge about military equipment to gain status, reputation, and recognition from others. Popescu insists he did not have the intention share state secrets with a foreign power. His goal was to show off his knowledge of technology, not to cause a security incident. Regarding the T-99 Panther documents, he stresses that these manuals are not part of the typical classification system for sensitive documents. Unlike standard state secrets, similar documents about other military vehicles are easily accessible online in forums, research archives, or unclassified repositories. He points out that even though the T-99 Panther manual was labelled "Confidential – restricted distribution," the information itself is available from other non-classified sources.

He believed that sharing it on a gaming forum did not meet the requirements to be labelled as a criminal act. Though technical manuals for military vehicles like the T-99 Panther can be found in various open sources, none have the specific label "Confidential – restricted

distribution" that this case involved. Popescu claims that his post did not give any strategic advantage to foreign powers; instead, it mainly sparked discussions on the forum and served as a way to display status.

The Vortex manual, in contrast, contains highly sensitive data and is under experimental classification. Popescu claims he was unaware of the extreme secrecy of the Vortex manual, believing it was a technical draft shared by mistake. The prosecution considers this as potentially more serious, but Popescu emphasizes that he had no intent to aid a foreign power, aligning with the pattern of recreational or accidental disclosure rather than espionage.

The prosecutor argues that the T-99 Panther manual was marked "Confidential – restricted distribution", and the Vortex manual was marked "Cosmic Top Secret". According to the law, sharing any classified information with a potential audience that includes foreign users can constitute the transmission of state secrets, regardless of the intent, if there is a risk of access by foreign powers.

The prosecutor emphasizes that intentional or not, the act created a situation where foreign powers could obtain sensitive military information, which aligns with the statutory description of treason. The defendant saw that the T-99 Panther manual was marked "Confidential – restricted distribution" and the Vortex manual as "Cosmic Top Secret", indicating awareness that the information had some level of state protection. This could be interpreted as reckless or negligent transmission of sensitive materials, supporting the prosecutor's case for treason.

The prosecutor argues that both manuals contain technical details about military systems, including operational capabilities, vulnerabilities, or experimental designs. In the prosecutor's view, even if Popescu's intent was to brag or impress forum members, the risk to national defence is significant, which aligns with the underlying purpose of article of the Penal Code that sanctions treason.

Types of documents that can be used as evidence

The evidence presented here is not exhaustive and represents fictional materials designed for the current exercise. The evidence can be expanded based on the intent of the participants and the duration of the case.

Computer Search Report – conducted by the cybercrime unit at the home of Andrei Popa. On 12.05.2025, a judicial search took place at the defendant's residence in Bucharest. The search was authorized by a warrant from the Bucharest Court of Appeal. During the search, the following items were seized: Dell laptop model XPS 15; External HDD - Seagate; USB flash drives: two units, 32GB each, Kingston; Printed documents representing copies of the T-99 Panther and Vortex manuals.

The laptop had several versions of the T-99 Panther manual, including one marked "Confidential, restricted distribution." The external hard drive contained a folder named "Military Manuals," which held the Vortex manual marked "Cosmic Top Secret." The USB flash drives had copies of both manuals, showing the defendant's intent to distribute the documents.

IT forensic report – an in-depth forensic analysis was done on the seized electronic devices. The analysis showed that multiple copies of the T-99 Panther manual were found on the laptop and external hard drive. Metadata indicates that the files were accessed and modified on 10.05.2025.

The Vortex Manual was located on the external hard drive, with metadata showing it was last accessed on 11.05.2025. The defendant's user account on the Taijiro Gaming forum was linked to the IP addresses tied to uploads of the sensitive manuals. The following forum logs were retrieved: - User Account: AndreiP - IP Addresses: 192.168.1.101 (Bucharest), 192.168.1.102 (Bucharest) - Posts: 10.05.2025: Uploaded T-99 Panther manual (Confidential) and 11.05.2025: Uploaded Vortex manual (Cosmic Top Secret) the logs confirm that the defendant's account was used to upload the sensitive manuals. This suggests unauthorized distribution of classified information. The T-99 Panther manual contains detailed specifications, operational procedures, and maintenance protocols for the tank. The Vortex manual includes classified information on experimental aircraft systems, flight dynamics, and weaponry.

Taijiro Gaming provided the following reports:

- Incident reports: previous instances of users uploading sensitive military documents, leading to temporary bans and content removal.

- Moderation logs: actions taken to remove unauthorized content and warn users about the consequences of posting classified materials.

Statements during hearings (examples):

- Defendant's Statement: "I uploaded the manuals to the forum to impress my peers. I didn't think it was a big deal. I didn't intend to harm national security."
- Witness Paul Ionescu, known on the forum as TBagGamerXXX0007: "I have known Andrei for years. He often brags about his knowledge of military technology. I believe he shared the manuals to gain respect in the community." The witness is a childhood friend of the defendant, who casually plays online games with him.

Requirements and questions of the case

The exercise is projected to last approximately one hour and the participants to must decide if the information leaked can be considered sensitive enough to be classified as treason case or an act of a lesser severity.

The participants must address the following issues regarding the case:

1. Did Andrei Popescu have the intent to transmit classified information to a foreign power, or was his motivation limited to forum bragging and status-seeking?

2. Considering that the materials were posted on a public gaming forum, does the potential accessibility of the manuals to foreign users constitute automatic transmission of state secrets, or is intent and actual harm required to establish treason?

3. The T-99 Panther manual was marked "Confidential – restricted distribution", while the Vortex manual was "Cosmic Top Secret". How does the difference in classification levels influence the legal assessment of Andrei Popescu's actions?

4. What role, if any, should Taijiro Gaming play in the case? Can the platform's previous incidents, moderation policies, and official statements about user-posted content affect the court's assessment of Andrei Popescu's responsibility?

References[1]:

1. Bodoroncea, Georgiana, Valerian Cioclei et al. (2020). *Codul penal. Comentariu pe articole [Criminal Code. Commentary on articles],* 3rd Edition, CH Beck.

2. Bomboy, Scott. (01.09.2023). *Aaron Burr's trial and the Constitution's treason clause*, National Constitution Centre.

3. *Cameron John Wagenius indictment,* (15.05.2025). https://www.justice.gov/opa/pr/former-us-soldier-pleads-guilty-hacking-and-extortion-scheme-involving-telecommunications.

4. Criminal Code of Romania – Law no. 286/2009, the updated version.

5. Criminal Procedural Code of Romania – Law no. 135/2010, the updated version.

6. Crane, Paul T. (n.d.). *Does the treason clause still matter? (Yes),* Interpretation & Debate, National Constitutional Centre. https://constitutioncenter.org/the-constitution/articles/article-iii/clauses/39#does-the-treason-clause-still-matter.

7. Dobrinoiu, Vasile, Pascu, Ilie, Hotca, Mihai Adrian et al. (2016). *Noul cod penal comentat. Partea specială [The new penal code commented on. The special part]*, 3rd Edition, Bucharest: Legal Univers.

8. European Court of Human Rights, Danilov v. Russia, case no. 88/05, (01.12.2020). https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-206264%22]}

9. European Court of Human Rights, *Nikitin v. Russia*, case no. 50178/99, (20.07.2004). https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-61928%22]}

10. Gadahn, Adam (Azzam al-Amriki) indictment, NSD (202) 514-2007. https://www.justice.gov/archive/opa/pr/2006/October/06_nsd_695.html

11. Korbein Schultz indictment, (23.04.2025). https://www.justice.gov/opa/pr/former-us-army-intelligence-analyst-sentenced-selling-sensitive-military-information.

[1] The exercise has been influenced by general events that have happened in democratic states. The exercise requires participants to understand, at a minimum, law enforcement legislation, cybersecurity provisions and human rights. In this regard, the author proposes the mentioned reading materials.

12. Larson, Carlton F.W. (2006). "The forgotten constitutional law of treason and the enemy combatant problem," *University of Pennsylvania Law Review*, Vol. 154, pp. 863-926;

13. Supreme Court of the United States of America, *case no. 325 U.S. 1 (1945),* 23.04.1945 decision, Cramer v. U.S.

14. Supreme Court of the United States of America no. 343 U.S. 717, (2.06.1952), Kawakita v. U.S.

15. *War Thunder's History of Classified Document Leaks*. https://blog.acer.com/en/discussion/3318/war-thunders-history-of-classified-document-leaks.

REVIEWS AND NOTES

Mihai Alexandrescu, (2024), *Leadership. Perspective teoretice [Leadership. Theoretical Perspectives]*, Presa Universitară Clujeană, Cluj-Napoca, 264p.,

presented by Claudia Anamaria IOV*

Mihai Alexandrescu's volume, *Leadership. Perspective teoretice [Leadership. Theoretical Perspectives]*, published in 2024 by Presa Universitară Clujeană, offers an exhaustive "conceptual map" essential for understanding and deepening one's grasp of leadership within the field of international relations and studies on organisations and institutions. From the very first pages, it becomes apparent that Alexandrescu seeks to make a well-founded and much-needed contribution to Romanian specialist literature, providing a comprehensive overview of the theoretical and historical evolution of the concept of leadership. From an analytical standpoint the volume aims to present an integrative vision of the main paradigms and schools of thought, from the earliest theories of charismatic leaders to the complex models of transformational and transactional leadership.

In his preface, Alexandrescu reveals that the purpose of this volume is to explore "some of the theoretical perspectives on this concept, offering readers an overview of the various theories and paradigms that have shaped our understanding of leadership to date" (p. 11). The book is grounded in a rigorously interdisciplinary analysis, well supported by an extensive bibliography and logically structured into four main parts (chapters): *Istoria și lexicul leadershipului [History and lexicon of leadership], Leadership ca persoană [Leadership type]*, *Leadership ca stil [Leadership style]* and *Leadership ca process [Leadership process]*.

* Lecturer, PhD., Department of International Studies and Contemporary History, Faculty of History and Philosophy, "Babeș-Bolyai" University, Cluj-Napoca, email: claudia.iov@ubbcluj.ro

The first part, *Istoria și lexicul leadershipului [History and lexicon of leadership]*, essentially serves as an introduction to the definition and evolution of the notion of leadership, aiming to familiarise readers, from an academic perspective, with the main concepts in this vast field and to establish key terms that underpin the explanations developed in the subsequent parts. The author's meticulous linguistic and historical research, supported by references to prominent scholars such as Richard L. Daft, Peter G. Northouse, and Roger Gill. He highlights the conceptual complexity of leadership and provides a robust foundation for understanding the transition from the classical paradigm, centred on stability, control, and hierarchy, to the modern one, oriented towards flexibility, collaboration, and continuous learning (pp. 18–20). At the same time, the analysis conducted throughout this first part, which undoubtedly required considerable research effort, successfully combines an accessible style with solid academic documentation, offering numerous examples from the political and managerial spheres, such as the case of former European Commission President Jean-Claude Juncker, used as a case study for adaptive leadership (p. 19).

A notable element of novelty, at least within Romanian specialist literature lies in Alexandrescu's original way of structuring the evolution of leadership theory into four major epochs: beginning with Era 1.0 of Heroic Leaders and concluding with Era 4.0 of Collaborative and Digital Leadership. By classifying and combining academic theories, this section underscores Alexandrescu's intention to contextualise them from a historical perspective. From a critical yet constructive point of view, one might note that it would be valuable to further analyse how the main leadership theories have been adopted and adapted within specific cultural or institutional contexts.

The second and third parts of the book, *Leadership ca persoană [Leadership type]*, *Leadership ca stil [Leadership style],* present the principal theories ranging from the "Great Man" model and trait-based approaches to behavioural, situational, transactional, and transformational theories. Throughout these sections, Alexandrescu addresses complex and essential themes in understanding the leadership process in an accessible language, introducing pedagogical innovations such as

"reflection themes" (pp. 72, 99, 112, 143, 169, 191, 206, 217, 228), which add a formative dimension to the volume and prove particularly useful for practitioners.

From a scholarly perspective, the volume illustrates a research endeavour developed over time and firmly grounded in strong theoretical documentation. In terms of how the concept of leadership is addressed, the author's main merit lies in his ability to concisely integrate the key theories and paradigms of the field, lending logical coherence to a concept that is inherently complex and multidimensional. The only possible critique of this work relates to its predominantly theoretical nature. While Alexandrescu provides a remarkable conceptual foundation, the inclusion of case studies, empirical applications, or correlations between theoretical models and contemporary examples from Romanian or European organisational contexts would have been highly beneficial. Such an applied dimension would have complemented the rich theoretical framework, granting the work additional practical value.

In conclusion, Mihai Alexandrescu's *Leadership. Perspective teoretice [Leadership. Theoretical Perspectives]* can be regarded as a reference work within the field of organisational studies in Romania. It presents a coherent and well-structured theoretical framework while opening avenues for further research particularly regarding the application of leadership models in diverse regional and institutional contexts.

GERMAN DEMOCRATIC REPUBLIC ESPIONAGE IN SCHLESWIG-HOLSTEIN

Helmut MÜLLER-ENBERGS

"The number of intelligence missions against Schleswig-Holstein that have been identified is well above the national average in relation to the population." (Constitution Protection in Schleswig-Holstein 1976)[1] This was stated by the State Office for the Protection of the Constitution in its 1976 annual report. Apparently, tranquil Schleswig-Holstein, one of the eleven federal states of the Federal Republic of Germany at the time, on the northern edge of the country, aroused the interest of foreign intelligence services, meaning those from the East. In 1978, it even stated: "The number of espionage cases increased significantly in Schleswig-Holstein in 1978. Over the last five years, there has been an

[1] Constitutional Protection in Schleswig-Holstein 1976, published by the Minister of the Interior of the State of Schleswig-Holstein in cooperation with the head of the press and information office of the state government (Schriften des Minister of the Interior, H. 19, Kiel 1977, p. 50), cited as: Constitution Protection in Schleswig-Holstein 1976.

increase of almost 100% in such cases" (Constitution Protection in Schleswig-Holstein 1978).[2]

Such statements do not allow any conclusions to be drawn about actual intelligence activities. They are merely "exact figures on solved cases" in order to "prevent enemy intelligence services from gaining insight into the extent of counterintelligence successes" (Constitutional Protection in Schleswig-Holstein 1978, p. 43). However, the 1978 report (p. 13) goes on to say: "Three quarters of all espionage activities in 1978 originated from intelligence services in the GDR." So even after the process of détente between the Federal Republic of Germany and the German Democratic Republic (GDR) that began in the 1970s, the intensity had by no means decreased, as had sometimes been assumed, according to the findings of the Office for the Protection of the Constitution (Constitution Protection in Schleswig-Holstein 1976, p. 50).

Judging by Table 1, Schleswig-Holstein did not enjoy a prominent position in the operational work of the Main Administration A (hereafter HV A) of the Ministry for State Security (MfS), which was responsible for foreign espionage, compared to the other federal states.

Table 1: Distribution of unofficial employees and contact persons of the HV A and its departments XV by federal state (as of December 1988) (Source: Helmut Müller-Enbergs: 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, 1998, p. 194)

Federal state	Unofficial employees and contacts	Percentage
Baden	13	7
Bavaria	241	13
Berlin	427	23
Bremen	30	2
Hamburg	102	5

[2] Constitutional Protection in Schleswig-Holstein 1978, published by the Minister of the Interior of the State of Schleswig-Holstein in cooperation with the Head of the Press and Information Office of the State Government (Schriften des Innenministers, H. 19, Kiel 1979, p. 13), cited as: Constitution Protection in Schleswig-Holstein 1978.

Hesse	140	7
Lower Saxony	134	7
North Rhine-Westphalia	462	25
Rhineland-Palatinate	43	2
Saarland	10	1
Schleswig-Holstein	53	3
Other	101	5

As of December 1988, HV A's operational centre was clearly located within Schleswig-Holstein, in the state's three largest cities – in order of size: Kiel, Lübeck and Flensburg. However, there is no mention of Neumünster, Norderstedt and Elmshorn, or even Wedel, Ahrensburg and Itzehoe. This is, as expected, evidence of a desire not to have an operational presence in all of the state's major cities. There are, however, special cases such as the small town of Rendsburg, which was home to the LANDJUT headquarters, the Army Air Defence School and other Bundeswehr facilities. The HV A listed five positions there in its statistics. And with this number of positions, the district of the Duchy of Lauenburg also counts as part of the affluent suburbs of Hamburg and Lübeck.

Table 2: Unofficial employees and contact persons of the HV A in Schleswig-Holstein (as of December 1988) (Source: Gunthar Latsch, Udo Ludwig: Fromme Spione, in: Der Spiegel, 65 (2011) No. 47, p. 44 f., here 45)

Location	Number
Lübeck	14
Kiel	9
Flensburg	7
Duchy of Lauenburg	5
Rendsburg	5
Pinneberg	4
Bad Segeberg	2
Husum	2
Ammersbek	1
Dithmarschen	1

Operational objectives of the HV A in Schleswig-Holstein

On 3 December 1979, various HV A units received Service Instruction No. 3 of 1979 from their headquarters in Berlin. It listed the individual operational objectives of the HV A that were to apply from then on, including those in Schleswig-Holstein.

In Kiel, the HV A wanted to maintain sources in the state government and the Ministry of the Interior, as well as in the fleet command in Flensburg-Mürwick and the Marienführungsdienstkommando (Marine Command) in Glücksburg-Meierwik. It also wanted to gain operational insight into the Kiel branches of the BND (Bundesnachrichtendienst), and the military counterintelligence service, the MAD (Militärischer Abschirmdienst), in particular their Group I. In Flensburg, the Federal Motor Transport Authority was also of interest.[3] Essentially, intelligence work was therefore concentrated in Kiel and Flensburg.

Responsibility for the individual targets was also regulated in these service instructions. According to internal guidelines, Schleswig-Holstein's Chekist mentor was therefore the HV A branch in Rostock, which operated as Department XV within the district administration (BV) of the MfS. The Rostock branch cooperated in part with the specialist departments of the HV A in Berlin, such as HV A IX, which was responsible for secret services and police, which is quite logical for the BND and MAD.

According to the planning documents of the HV A, its service unit in Rostock was assigned the key role for operational work in Schleswig-Holstein. So let us ask: Did this also correspond to operational practice? A compilation of the operational procedures carried out by the HV A in Schleswig-Holstein clearly shows the prominent role played by the Rostock Chekists. No fewer than six Schleswig-Holsteiners were registered for this service unit. But the neighbouring district branches of the HV A, such as Schwerin and Neubrandenburg, are only slightly behind the responsible service unit. This even applies to a lesser extent to Magdeburg and the more distant Leipzig. Consequently, Service

[3] See Helmut Müller-Enbergs: Hauptverwaltung A. Aufgaben – Struktur – Quellen (Headquarters A. Tasks – Structure – Sources), Berlin 2024, p. 307.

Instruction No. 3 from 1979, which was intended as a control measure, only fulfilled its function to a limited extent. The service units – even the specialist departments at headquarters in Berlin – recruited whatever they could find. The plan did not succeed. Instead, quite a few of the HV A service units ended up in Schleswig-Holstein: a third of the district branches and soon half of the central specialist departments.

The network of intelligence positions of the HV A in Schleswig-Holstein did not emerge overnight, but was rather the product of a long development process. This can only be partially captured by the snapshot taken in December 1988. After all, the 51 unofficial employees (IM) and contact persons (KP) of the HV A in Schleswig-Holstein included 18 women, which is a comparatively above-average proportion of 35 per cent. Not quite, but soon half of the operational heaven belonged to women in Schleswig-Holstein. The youngest among them was 25 years old on the cut-off date, the oldest 74. More than half of the HV A's active members were born between 1930 and 1939 (n = 15) and between 1940 and 1949 (16), had reached or already passed the age of 50, and were shaped by a childhood under National Socialism or the post-war period and the emerging affluent generation (Müller-Enbergs, 1998). Seven confidants of HV A were in their sixth or seventh decade of life and were still influenced by the Weimar period. Viewed in this light, the operational network appears to be ageing – and the next generation was slow in coming. Only four citizens were between 25 and 28 years old, while eleven were between 30 and 39. The prognosis of an ageing operational network in Schleswig-Holstein can be derived from the recruitment years themselves. Well over half (n = 31) of the citizens active for the HVA in Schleswig-Holstein in December 1988 had committed themselves to cooperation between the ages of 17 and 38 (Müller-Enbergs, 1988). While the HV A was recently only able to recruit four citizens between the ages of 25 and 28, at least implicitly, in previous years – according to the most recent active members – there had been more than three times as many (n = 13), including a remarkably high number of eight women (Müller-Enbergs, 1988).

Some of the Schleswig-Holsteiners led by the HV A have been active for a long time. Seven of them had already been active for over twenty years, and another 14 for between ten and twenty years. In any

case, there were recruitment gaps in the years from 1962 to 1967 due to the construction of the Berlin Wall (Müller-Enbergs, 1988). Even in the second half of the 1970s, only one Schleswig-Holstein resident remained in the HV A networks. This changed in the 1980s, when an average of three to four people took the bait each year, but these included quite a few who had already reached a considerable age. It can be assumed that, in quantitative terms, the HV A network in Schleswig-Holstein had passed its operational zenith. The statisticians within the HV A will certainly have called for increased recruitment efforts.

The HV A had operated as one of the MfS's service units in Schleswig-Holstein. In December 1988, there were 51 unofficial employees and contact persons on record, including ten sources in target objects (Müller-Enbergs, 1988). According to current knowledge, it only achieved its ambitious goals of infiltrating the state government and the Ministry of the Interior of Schleswig-Holstein to a limited extent. It was able to achieve other operational goals, such as the Federal Motor Transport Authority in Flensburg, but was clearly not present in others at the time of the investigation.

The unofficial network in Schleswig-Holstein was getting old, and the HV A was having difficulty recruiting new members. Although it had a considerable logistical apparatus at its disposal – from border smugglers to conspiratorial apartments – it found it difficult to consistently pursue its planned objectives, even though there were some promising contacts in the end. The local deployment and the operational sources under contract sometimes appear arbitrary. Recently, the journalist "Bernhard" provided significant political access to the state government, and the politician "Hecht" provided a possibly unconscious skimming contact. At least from the HV A's point of view, the HV A's foreign intelligence service was far from having infiltrated Schleswig-Holstein. Furthermore, the HV A only partially succeeded in achieving its operational goals in Schleswig-Holstein.

*

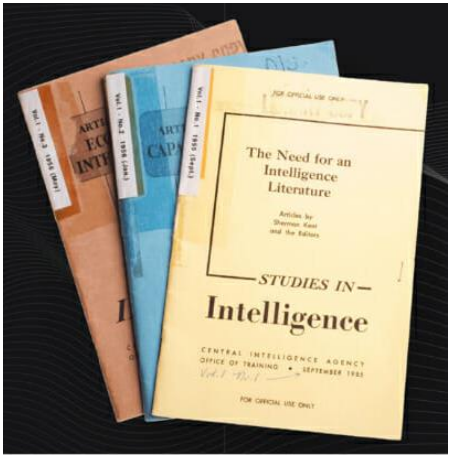
For more details about this espionage network see the volume edited by Nils Abraham, Thomas Wegener Friis, Helmut

Müller-Enbergs[4], Mogens Rostgaard Nissen, *Spionage im Grenzland Nachrichtendienste in Schleswig-Holstein und Süddänemark* [*Borderland Intelligence Services Espionage in Schleswig-Holstein and Southern Denmark*], BeBra Science Publishing House, Berlin, 2025, 336 p.[5] The contributions in this volume focus for the first time on this invisible history in the German-Danish border region from a broad temporal perspective: during the First World War, during the Nazi era and the German occupation of Denmark in the Second World War, as well as during the Cold War after 1945. Thus, the volume makes a contribution not only to regional history, but also to international intelligence history.

The volume was possible with the contribution of sixteen authors: Nils Abraham, Dieter Bacher, Kristian Bruhn, Wladyslaw Bulhak, Martin Göllnitz, Bodo v. Hechelhammer, Anne Heckmann, John Jensen, Henrik Lundtofte, Carsten Müller-Boysen, Helmut Müller-Enbergs, Anne Rheder Andersen, Mogens Rostgaard Nissen, Jon Thulstrup and Thomas Wegener Friis.

[4] Helmut Müller-Enbergs is an associate professor at the Cold War Centre at the University of Southern Denmark, email: mueller.enbergs@googlemail.com. He worked for over two decades as a senior researcher at the Federal Office for the Stasi Archive and is one of the leading experts on the history of the East German foreign intelligence service. See more on https://mueller-enbergs.de/92/vita

[5] More details on: https://bebra-wissenschaft.de/vzgesamt/titel/spionage-im-grenzland.html



STUDIES IN INTELLIGENCE 70 YEARS OF THE CIA'S FLAGSHIP PROFESSIONAL JOURNAL

presented by Dan ROMAN

September 2025 marks the 70th anniversary of *Studies in Intelligence*[1], the CIA's authoritative publication dedicated to the art and science of intelligence**.** Since its founding, the journal has stood the test of time as a platform dedicated to reflection, debate, and the transmission of lessons learned within the intelligence profession. Over the decades, it has become not only a landmark for the American intelligence community but also a valuable source for scholars and practitioners worldwide. Through its articles, *Studies in Intelligence* has managed to bridge theoretical reflection with the practical lessons of intelligence work, contributing decisively to the consolidation of a professional culture based on learning, history, and institutional memory.

Origins and mission

The creation of the journal is closely linked to the vision of Sherman Kent**,** regarded as "the father of intelligence analysis". Coming from an academic background (he was a history professor at Yale), Kent

[1] Please see the collection of the journal on the official website. The source for the image is https://intelligencestudies.utexas.edu/news/isp-director-s-essay-on-intelligence-integration- in-studies-in-intelligence/

believed that the success of intelligence work required more than clandestine operations or the collection of raw data. For him, the key lay in developing a solid conceptual and methodological foundation for analysis.

Thus, in 1955, he initiated *Studies in Intelligence* as an in-house journal designed to encourage critical reflection on intelligence practice, stimulate the exchange of ideas among professionals, and preserve experiences and lessons learned. From the outset, its mission was clearly defined**:** "to contribute to the understanding, improvement, and transmission of the art and science of intelligence." More than a professional publication, Kent envisioned a body of specialized literature that, at that time, was virtually non-existent.

Structure and content

The journal is published quarterly and includes articles covering a wide range of topics:

- ✓ intelligence analysis – methodologies, forecasting techniques, comparative evaluations;
- ✓ operations and clandestine practices – generally presented as historical studies or lessons learned from past experiences;
- ✓ technology and innovation – the role of new tools in the collection and processing of information;
- ✓ the history of intelligence – case studies on the Cold War, regional conflicts, or key moments in the evolution of the CIA and other services;
- ✓ book reviews – designed to maintain the connection between the intelligence community and the relevant academic and literary environment.

Although a significant portion of the content is classified and circulates only within the American intelligence community, the CIA also publishes an unclassified edition of the journal, available to the general public on its official website. This edition allows researchers, journalists, and practitioners from other countries to gain a better understanding of the theoretical and methodological concerns of American intelligence.

The role in the CIA's professional culture

In an organization where secrecy is the rule, *Studies in Intelligence* has become a controlled but essential space for institutional self-reflection. The publication encourages the analysis of both successes and failures in a manner that allows organizational learning and helps avoid repeating mistakes.

Moreover, the journal reinforces the idea that intelligence is not merely a technical activity, but also an intellectual endeavor that requires the development of critical thinking, argumentative skills, and a constant dialogue between practitioners and theorists. In this sense, *Studies in Intelligence* plays a role similar to that of academic journals in political science or strategic studies, while remaining deeply rooted in the practice of intelligence services.

Through its open edition, *Studies in Intelligence* has become an important source for researchers worldwide. Numerous academic works on the history of the CIA, on strategic analysis, or on forecasting methodologies cite articles published in this journal.

In addition, the articles published between 1955 and 1991 are available almost in their entirety through the *CIA Reading Room* or, more simply, on the National Archives and Records Administration (NARA) website, offering access to a particularly valuable archive for research into the history of American intelligence.

For the international intelligence community, *Studies in Intelligence* provides a model of selective transparency and continuous professionalization. The fact that the CIA has chosen to share part of its reflections and lessons with the broader public demonstrates not only its desire to build a positive institutional image but also its conviction that a modern intelligence service must engage in dialogue with society and with the academic environment.

Relevance in the context of the development of intelligence studies

Internationally, there is a growing trend in the development of intelligence studies as an academic and professional discipline. In universities, research institutes, and practitioner communities, intelligence is analyzed from multiple perspectives: historical, methodological, technological, and ethical.

In this context, *Studies in Intelligence* plays the role of a catalyst, offering a model of institutional reflection and serving as a bridge between secret practice and open debate. The lessons and approaches promoted in its pages can inspire not only American professionals but also academic communities and intelligence organizations around the world, which are in a continuous process of consolidation and modernization.

Conclusions

After seven decades of uninterrupted publication, *Studies in Intelligence* continues to stand as a central pillar in the professional architecture of the CIA. The journal has consistently demonstrated that intelligence is not confined to clandestine operations or secret reports, but is also an intellectual discipline with its own methods, theories, and debates. Seventy years on, it remains a unique forum for critical reflection and institutional learning, a bridge between past lessons and future challenges. For readers and researchers, CIA's *Studies in Intelligence* offers a rare window into how the world's most renowned intelligence agency cultivates its memory, strengthens its professional culture, and prepares for the uncertainties ahead. More than a publication, it is a laboratory of ideas that shows how national security is built not only through action, but equally through reflection.[2]

References:

1. Unclassified edition of *Studies in Intelligence*: CIA.gov – Studies in Intelligence.

2. Historical archive (1955–1991), available through the *CIA Reading Room*.

3. *National Archives and Records Administration (NARA):* NARA – Studies in Intelligence.

[2] Dan Roman is an associate assistant within the Western University "Vasile Goldiş" of Arad, email: roman.dan@uvvg.ro.

ACADEMIC FOCUS

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

In July 2025, "Mihai Viteazul" National Intelligence Academy (ANIMV) completed its 5th academic mobility project (KA131_2023) dedicated to the countries participating in the ERASMUS+ programme. Through the Erasmus KA_131 mobility project won in 2023, ANIMV set out to continue the efforts started in 2018 towards institutional internationalization and the development of the key competencies and skills of teaching/administrative staff and students from our academic study programs, through all 4 types of mobilities – study, practice, teaching and training. Additionally, we considered increasing and expanding university partnerships with universities from participating countries. Upon finishing the 26 months of implementation, ANIMV has managed to consolidate its status as a trusted European partner and higher education institution focused on the development of students and staff, evidenced by the following academic milestones derived from the set objectives:

1. supporting four participants in order to develop key competencies and promote lifelong learning;

2. increasing ANIMV's visibility among the European university community and facilitating the exchange of good academic practices with higher education institutions with similar profiles and training centers with a tradition in the area of training courses for professionals;

3. promoting diversity, inclusion and equal opportunities by organizing four outgoing mobilities, one for each of the four categories;

4. developing the capacity to offer study programs better oriented towards the European community – introducing new subjects taught in English, rethinking a Master's degree program in order to increase its attractiveness – creating synergies with other Erasmus projects carried out within ANIMV (INSET – Erasmus Mundus Design Measures);

5. intensifying the digitalization process by transposing courses and support materials used in the traditional setting to the digital classroom;

6. mapping new possible funding opportunities offered within the framework of the Erasmus program and preparing project proposals with partners to create additional academic synergies.

In conclusion, the KA131_2023 project represented another essential step in consolidating ANIMV's internationalization process, with direct effects on the quality and relevance of the educational databases offered within the academic study programs. During the implementation period the Academy reconfirmed its capacity to capitalize on opportunities for training, exchange and European cooperation, generating a visible impact on the development of the skills of teaching/ administrative staff and students, and at the same time contributing to the consolidation of its position as a trusted partner and learning/ research hub. As a result, due to this solid foundation, the Academy will be able to build and expand future university partnerships, both in the area of classic university mobilities and in the area of broader projects.

Collectively, the five ERASMUS+ projects that have been implemented so far have encompassed a number of 18 beneficiaries, students and professors alike, who took part in different types of mobilities, as follows:

- 7 training mobilities;
- 5 traineeships;
- 3 teaching mobilities;
- 3 study mobilities.

ANIMV is currently implementing two more Erasmus+ KA131 mobility projects for which it has received funding under the 2024 and 2025 calls, respectively.

Prevention of Weaponization and Enhancing Resilience against Security-related Disinformation on Clean Energy – POWER
Grant agreement no. 2024-1-RO01-KA220-HED-000245038
(2024 – 2027)

POWER Project addresses the fight against climate change by mitigating the effects of clean-energy-related disinformation on public policy adoption and implementation among both the target group and the general public. The project directly tackles two crucial societal challenges: climate change and the pervasive issue of disinformation, particularly around renewable energy. By engaging students, educators, and professionals across Romania, Malta, Spain, and Moldova, it aims to elevate media and clean energy literacy, foster a comprehensive understanding of environmental issues, thus enhancing resilience against disinformation.

The project consortium is headed by "Mihai Viteazul" National Intelligence Academy and the partners are University Rey Juan Carlos, Spain, the University of Malta, Eurocomunicare Association. The project also has an associated partner The Center for Strategic Communication and Countering Disinformation, in the Republic of Moldova.

The project's first general objective is to facilitate transition to clean energy by fostering an informed fact-based public discussion on clean energy sources. In correlation, the second general objective is to strengthen societal resilience against the weaponisation of clean energy conversations by disinformation actors, and to contribute to the EU's policy objectives to reduce net greenhouse gas emissions by 55% by 2030 and to generate at least 42.5% of the EU's energy from renewable sources.

These objectives have been broken down into six specific objectives: (1) to develop a lexicon related to clean energy and associated

concepts in Romania, Spain, Malta and the Republic of Moldova in the target languages; (2) to map online disinformation modus operandi, techniques, and narratives in the four participating countries. The project will collect and analyse automatically and manually clean-energy-related disinformation narratives on three social media platforms. The results of both these research activities will represent the basis of the clean-energy lexicon; (3) to neutralize clean energy disinformation through dynamic science communication in Romania, Spain, and Malta; (4) to enhance clean energy and media literacy among students, teaching staff and employees of the partner organizations. These results will be achieved through organizing three, five-day, face-to-face Clean Energy Cafes as learning events which bring together students in the fields of security, intelligence, communication, social sciences, and sciences with teaching staff and employees in the same areas and are designed as experiential, learning-by-doing activities; (5) to foster a collaborative empowered community of practice among students in the partner organizations and local universities by organizing four three-day face-to-face Clean Energy Living Labs dissemination activities in each partner country. In these labs, participants will work together to design innovative, artistic, digital productions to increase clean energy literacy and preempt disinformation; (6) to create and populate digital educational content and tools addressed to stakeholders in the four partner countries. This e-learning hub will include a Practitioner's Digital Briefcase, an Educator's Digital Briefcase, digital storylines, online learning modules. These will foster the development of new teaching and learning practices through digital content and interactive learning resources.

At the heart of this initiative is the development of innovative educational content and digital tools. This includes a clean energy lexicon, immersive learning scenarios, and digital storylines, all designed to debunk myths perpetuated by disinformation campaigns about renewable energy. The approach integrates cutting-edge research, participatory teaching methodologies, and broad dissemination activities, such as Clean Energy Living Labs and Clean Energy Cafés.

Key to the strategy is the cross-sectoral collaboration that leverages the expertise of the partner organizations with a proven track record in digital education, fighting against disinformation and environmental projects. By creating synergies between media literacy, environmental education, and digital pedagogy, POWER not only addresses the selected priorities head-on but also pioneers a holistic model for tackling complex global challenges.

EU Knowledge Hub on Prevention of Radicalisation (EUKH)

The EU Knowledge Hub on the Prevention of Radicalisation takes up the legacy of the Radicalisation Awareness Network and aims to provide a set of resources and activities such as trainings, workshops and study visits, as well as mentoring and job shadowing for young professionals in the field of preventing and combating radicalisation. Further, selected experts will conduct research on specific topics in line with the project's general objectives. Two communities of experts will support the project: The Knowledge Hub Research Committee, composed of 15 internationally recognised researchers in the field and the EU Research Community on Radicalisation (ERCOR), a database of experts which will be called upon when their expertise is required.

The activities of EUKH will be grouped according to several thematic panels, which will represent the main directions of the projects and will be aligned with the priorities set out in the Strategic Orientations. The thematic panels will be composed of leaders and co-leaders, selected from the expert database, as well as invited researchers. The results of the activities of thematic panels will be summarized in annual reports.

Further, EUKH will offer tailor-made support services, requested by a member state, with the aim for addressing specific challenges in the field of combatting radicalisation. These tailor-made support services will assist Member States to implement EUKH results to their specific conditions.

The project was selected through a competitive tender organized by the European Commission. The project will be conducted over four years and has a total budget of 60 million Euros. The winning consortium is led by NTU Denmark and is composed of "Mihai Viteazul" National Intelligence Academy (MVNIA), IPS Innovative Prison Systems (Portugal),

Polish Platform for Homeland Security, Fundación Euroárabe (Spain), Center for Security Studies (KEMEA – Hellenic Ministry of Citizen Protection), Hellenic Foundation for European and Foreign Policy, European Research and Project Office (EURICE, Greece), Deep Blue, European Centre of Studies and Initiatives (CESIE, Italy).

Romania is represented by the "Mihai Viteazul" National Intelligence Academy, which will support training and research activities on the process and factors supporting radicalisation. It will also incorporate research findings in its B.A., M.A. and PhD curricula, as well as support the development of a common culture among practitioners dedicated to combating radicalisation.

INTERconnected Security Operation Centres – INTERSOC Strengthening Europe's cybersecurity infrastructure through innovative machine learning solutions and collaborative intelligence[1]

(January 2024-January 2027)

The Romanian National Cyber Security Directorate (DNSC) is the beneficiary of a grant for the implementation of the **project INTERconnected Security Operation Centres – INTERSOC,** under financing contract no. 101145853. The project is funded by the Directorate-General for Communications Networks, Content and Technology CNECT.H – Digital Society, Trust and Cybersecurity, H.1 – Cybersecurity Technology and Capacity Building, under the call for projects DIGITAL-ECCC-2022-CYBER-B-03, type of action: DIGITAL-JU-SIMPLE.

Cyber threats have a global impact, often going beyond sectorial borders and producing far broader effects than the targets initially settled. In a context where digital systems are becoming increasingly complex, total prevention of cyber-attacks is no longer possible. However, through robust, integrated and coordinated defence mechanisms, risks can be significantly reduced, ensuring critical infrastructure protection

[1] We thank PhD Claudia Lascateu for the presentation. The INTERSOC project received funding from the Directorate-General for Communications Networks, Content and Technology CNECT.H – Digital Society, Trust and Cybersecurity, H.1 – Cybersecurity Technology and Capacity Building, under grant contract No 101145853. However, the opinions expressed belong exclusively to the author(s) and do not necessarily reflect the views of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.

and business continuity. Currently, cybersecurity efforts in the European Union are often fragmented, while cyber-attackers are increasingly coordinated and sophisticated. This reality calls for a new approach to the protection of critical infrastructures. Monitoring the tactics, techniques and procedures used by malicious actors, together with analysing their motivations and targets, can help improve incident detection and response capabilities.

The INTERSOC project was designed to strengthen the level of cybersecurity across the European Union. The initiative aims to increase preparedness at national and European level, facilitate advanced threat forecasts, strengthen cyber incident detection and response capabilities and develop skills in the security of digital infrastructures, while respecting privacy principles and fundamental rights.

Coordinator: Eximprod Engineering S.A. – EPG – Romania. Partners: Aristotelio Panepistimio Thessalonikis (AUTH) – Greece; Asm Terni Spa (ASM) – Italy; Caixabank SA (CAIXA) – Spain; Ethniko Kentro Erevnas Kai Technologikis Anaptyxis (CERTH) – Greece; Clone Systems Cy Ltd (CLONE) – Cyprus; Cyberethics Lab Srls (CEL) – Italy; Diethnes Panepistimio Ellados (IHU) – Greece; SQS Business Services SRL – Romania; Southeast Electricity Network Coordination Centre Selene Cc Anonymi Etaireia (SELENE) –Greece; Sphynx Hellas Anonymi Etaireia (SPH) – Greece; National Cyber Security Directorate (DNSC) – Romania. Affiliated entity: Frontiere – Italy.

As cyber-attacks become increasingly sophisticated, multidimensional and difficult to detect by traditional means, these threaten not only the continuity of essential services, but also the economic and social security of the European Union. In this context, it is essential to develop innovative solutions capable of providing advanced threat forecasting, improved detection and response capabilities, as well as tools for secure collaboration between institutional and private actors in the field of cybersecurity. The INTERSOC project responds to these challenges through an integrated and user-centred approach, combining state-of-the-art technologies with advanced information sharing mechanisms.

The overall objective of the INTERSOC project is to *strengthen cybersecurity incident response and increase the resilience of digital infrastructures* by developing advanced threat forecasting, detection and incident response capabilities at national and European levels. In parallel, the project aims to strengthen skills through dedicated training sessions on the security of digital infrastructures. The INTERSOC project also aims to strengthen a resilient, safe and sustainable European cybersecurity ecosystem based on trust, cooperation and compliance with the evolving European regulatory framework.

The specific objectives of the project relate to:

- **Monitoring of complex network and information systems.** The project will develop advanced monitoring mechanisms for complex network and information systems capable of identifying anomalies caused by advanced, multidimensional cyber-attacks. This will be achieved by extending traditional SIEM (Security Information and Event Management) and IDS (Intrusion Detection Systems) functionalities with behavioural and decision-making artificial intelligence algorithms, enabling faster and more accurate incident detection.
- **Low-code approach to security and automation of cyber incident management.** INTERSOC will implement a low-code/no-code approach that will enable a flexible and scalable approach to security processes and incident management automation. This will reduce human intervention, speed up response times and improve the resilience of Security Operation Centers (SOCs).
- **Decentralised and Confidential Sharing of Cyber Threat Information (CTI).** The project will develop a decentralised and confidential mechanism for cyber threat information sharing based on peer-to-peer networks aligned with the European regulatory framework (NIS2, GDPR and related regulations). This will strengthen cross-border and inter-institutional cooperation, enabling a secure and reliable exchange of information.
- **Reliable solutions and technologies for information exchange.** INTERSOC will design and refine trusted solutions and technologies

to address challenges related to establishing and maintaining trust between partners during online information sharing. They will create a secure and transparent collaboration framework, reducing the risks of data manipulation or compromising information flows.

- **Risk and threat analysis, impact assessment and mitigation.** An important objective of the project is to identify, analyse and mitigate vulnerabilities in pilot systems through specific activities. This integrated approach will ensure a high level of security and help strengthen the resilience of the pilot infrastructures tested.
- **Advanced Penetration Test Tools and Methodologies.** Advanced tools and methodologies on penetration testing for new vulnerabilities will be developed and tested. They will be actively tested in SOCs (Security Operation Centres) as part of pilot tests, simulating real cyber-attacks and testing the ability to defend infrastructures.
- **Reliable artificial intelligence algorithms.** The project will develop trustworthy AI algorithms in line with European AI regulations (e.g. proposed AI Act), aligned with relevant standards and working groups (e.g. CEN/CLC JTC21 WG4). These algorithms will comply with transparency, ethics and traceability requirements, while ensuring enhanced performance.
- **Cyber Range Platform for Advanced Exercise.** INTERSOC will use a virtualization platform to host and conduct advanced red team/blue team exercises. These cyber exercises will strengthen institutional capacities, provide realistic training environments and increase users' awareness and preparedness.
- **Validation in three pilot sectors (banking, energy, CSIRT-Cyber Security Incident Response Teams training)**

The project results will be validated through case studies and practical scenarios in three representative sectors:

- the banking sector, where customer security and trust are essential;
- the energy sector, which is essential for economic stability and the functioning of society;

- training and training of CSIRTs, for which knowledge transfer and practical training are fundamental for rapid response to cybersecurity incidents.

Through its approach, the INTERSOC project aims to manage the most important challenges of cybersecurity at European level, including threat forecasting and the development of response capacities:

- **Prediction of threats.** Implement advanced machine learning models, capable of predicting with high precision the evolution of cyber threats, supporting the adoption of proactive defence measures and increasing the resilience of European critical infrastructures.
- **Integration of SOC.** Creating an interconnected network of Security Operations Centres (SOCs), capable of sharing threat intelligence, coordinating responses and providing mutual support in real time.
- **Automated response.** Implement automated incident response systems capable of responding to threats in a shorter time than human operators, minimising the impact, damage and length of the recovery process.
- **Information sharing** (Knowledge exchange). Establish standardised protocols to facilitate the exchange of information on cyber threats and best practices between participating organisations and states, helping to increase trust and build collective resilience.
- **Capacity building.** Increase European cybersecurity capabilities through training programmes, knowledge transfer and the development of a new generation of security professionals.

Through these strategic directions, INTERSOC project aims to strengthen a safer, more resilient and better prepared European cybersecurity ecosystem for the challenges of the future. The integrated approach – from threat prediction and automated response to information exchange and human resources development – reflects the shared commitment to improve European cooperation to a competitive and security advantage in the face of an increasingly complex digital environment.

INnovative multi-diSciPlinary Industry-focused cybersecurity education for upskilling and ReskIlling the EU workforce – EU-INSPIRE[2]

(January 2025-January 2028)

The Romanian National Cyber Security Directorate (DNSC) is the beneficiary of a non-reimbursable financing for the implementation of **INnovative multi-diSciPlinary Industry-focused cybersecurity education for upskilling and ReskIlling the EU workforcE– EU-INSPIRE** project, under the grant agreement no. 101190054. The project is financed through Digital Europe Programme by the granting authority: European Health and Digital Executive Agency (HaDEA), under the call DIGITAL-2023-SKILLS-05-SPECIALEDU – Specialised Education Programmes in Key Capacity Areas topic, type of action: DIGITAL Lump Sum Grants.

The EU-INSPIRE project responds to the urgent need to bridge the cybersecurity skills gap across the European Union and to train a new generation of professionals with advanced expertise in the political, organisational and technological dimensions of cybersecurity and artificial intelligence (AI). As the cyber threat landscape evolves, specialised training programmes capable of up skilling and reskilling

[2] We thank PhD Claudia Lascateu for the presentation. EU-INSPIRE project has received funding from the European Union's Digital Europe Programme, DIGITAL-2023-SKILLS-05 call, under the Grant Agreement no.101190054. Views and opinions expressed are however those of the author(s) only, and the European Union or the granting authority is not responsible for any use that may be made of the information it contains.

the workforce are essential to ensure the resilience of Europe's digital infrastructures and services.

Launched in January 2025 with a funding of 19,477,569.31 euro of which non-reimbursable financial assistance of 9,638,686.15 euro, the project will be implemented over a period of 48 months and will aim to develop a sustainable and multidisciplinary cybersecurity education ecosystem. Accredited and certified training programmes will also be developed, a cybersecurity campus will be created, and the foundations of the EU-INSPIRE Academy will be laid.

The Consortium, consisting of 24 partners from 14 European countries, is coordinated by the University of Piraeus Research Center (Greece) and includes top academic institutions, research organisations, private companies and national authorities: Mib Developpement Ecole des Ponts Business School – France; Universitetet I Oslo – Norway; Technische Universitaet Muenchen – Germany; Universidad De Malaga – Spain; Anoikto Panepistimio Kyprou (Open University of Cyprus) – Cyprus; Consiglio Nazionale Delle Ricerche – Italy; Euroopan Hybridiuhkien Torjunnan Osaamiskeskus – Finland; United Nations Interregional Crime And Justice Research Institute – Italy; Bitdefender SRL – Romania; Obrela Security Industries – Ypireseies Asfaleias Pliroforion Anonymos Etaireia- Greece; Sphynx Hellas Anonymi Etaireia – Greece; Cyberalytics Limited – Cyprus; Insuretics Limited – Cyprus; Karavias Mesites Asfaliseon Kai Symvouloi Asfaliseon Anonymi Etairia – Karavia Insurance Brokers And Insurance Advisors Societe Anonyme – Greece; Asfalys SRL – Belgium; Eunomia Limited – Ireland; AEGIS IT Research GMBH – Germany; Cardet Centre For The Advancement Of Research & Development In Educational Technology Limited – Cyprus; Circular Economy Foundation – Belgium; Cyprus Organisation For Standardisation – Cyprus; Balgarska Organizatsia Po Kibersigurnost Sdruzhenie – Bulgaria; Directoratul National De Securitate Cibernetica – Romania.

The overall objective of the EU-INSPIRE project is to revolutionize the landscape of higher education within the cybersecurity domain by cultivating new group of specialists, equipped with master-level expertise across the political, organizational, and technological dimensions of

cybersecurity, artificial intelligence (AI), and cyber insurance. Its goal is to shape an advanced educational ecosystem that not only fosters the development of specialized skills but also supports the continuous up skilling and reskilling of professionals in response to evolving industry demands and challenges. During its lifetime, the project will deliver three distinct master's programs (MSc, MBA, and MSc by research) and will engage over 1,000 students in master's programmes and award 5,000 certifications, creating a lasting European education program that trains cybersecurity experts, keeps their skills current, and makes sure everyone has access to quality training that matches what employers need.

EU-INSPIRE's mission is to respond to the need for addressing the multifaceted educational and vocational training needs critical to support the future EU Cyber Resilience ecosystem through an innovative three-fold approach:

- nurturing ICT personnel adept in leveraging AI-driven cybersecurity technologies to enhance the resilience of processes, systems, and digital infrastructures,
- cultivating cyber insurance specialists who possess a deep understanding of how cybersecurity and AI converge to protect cyber insurance policies, alongside expertise in deploying mechanisms for the assessment of cyber risks and threats, and
- empowering domain experts with sector-specific insights into digital transformation, who are proficient in applying cutting-edge AI solutions to cybersecurity conformity assessments. EU-INSPIRE is set to implement strategic mechanisms aimed at engaging a diverse array of industrial and research-driven communities ensuring the sustainability of the ecosystem beyond the end of the project through the development of a financially viable and cost-effective roadmap for establishing the EU-INSPIRE Academy. This institution is envisioned to serve as a cornerstone of the next-generation EU Cybersecurity Foundation, fostering synergies and integration with existing EU commitments aimed at mitigating the cybersecurity skills gap.

As partner in the EU-INSPIRE project, DNSC will ensure the coverage of the curricula with respect to policies and the compliance of the certifications to proposed policy recommendations. Highlights: (i) expertise in cybersecurity standards, regulations, and best practices; (ii) guidance on curriculum alignment, certification pathways, and industry accreditation, facilitating students' seamless transition into the workforce; (iii) hubs for technological innovation and entrepreneurship; (iv) expose students to emerging technologies, research collaborations, and industry partnerships; (v) access to state-of-the-art facilities, mentorship programs, and networking opportunities, fostering a culture of innovation and entrepreneurship among students.

The project directly contributes to achieving the Digital Decade targets and Europe's Digital & Green Transition by enhancing the security level of data and e-services operated by EU organisations, boosting economic growth for EU companies, facilitating the swift transition to digital transformation, expanding opportunities for students and professionals seeking careers in cybersecurity, providing top-notch training opportunities for students from various sectors and cultural backgrounds, and ensuring inclusiveness through Educational Mobility Grants that prioritize students with disabilities and those from low socio-economic backgrounds.

Funded by the European Union

Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe – ENDURANCE

Grant agreement no. 101168007

The Romanian National Cyber Security Directorate (DNSC) is the beneficiary of a non-reimbursable financing for the implementation of the **Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe – ENDURANCE** project, under the grant agreement no. 101168007. The project is financed through Horizon Europe Programme, by the granting authority: European Research Executive Agency (REA), under the call HORIZON-CL3-2023-INFRA-01 topic, type of action: HORIZON Innovation Actions[3].

Amidst an increasingly interconnected and complex world, the provision of essential services remains crucial for the well-being of European citizens and the smooth functioning of the internal market. Yet, the ever-evolving landscape of risks, ranging from cyber threats, physical attacks, and human errors to natural disasters, demands a proactive and collaborative, pan-European approach to ensure disruption resilience. ENDURANCE is driven by the critical need to fortify Europe's essential services against potential disruptions, transcending the sole focus on the underlying critical assets.

Recognizing the significance of the Critical Entity Resilience (CER) and NIS2 Directives in setting the groundwork for resilience and, in

[3] We thank PhD Claudia Lascateu for the presentation. The ENDURANCE project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement no. 101168007. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

parallel, the current silo approach to the Critical Infrastructure (CI) resilience and business continuity of essential services they provide, the project will assist the CI authorities across Europe in fully grasping and harmoniously implementing both directives.

To maximize the impact of our developments and projects' results, the Pan-European Working Group on Disruption Resilience (WGDR) will be created. The main direction of this expert networking is an information exchange ecosystem to feed the Critical Infrastructure Stakeholders' community with relevant best practices and new knowledge on improving the resiliency of their infrastructure. The ENDURANCE project responds to this need by bringing together a consortium of 23 partners from 7 European countries, which includes 7 authorities, 5 critical infrastructure operators from 6 key sectors and 11 entities with expertise in different domains. With a 36 months duration, launched in October 2024, this 5-million-euro EU-funded initiative is committed to developing interoperable solutions aimed at strengthening Europe's defences. The project will deliver robust methodologies, cutting-edge technologies, and strategic frameworks to build the resilience of critical infrastructures and ensure their capacity to recover from both physical and cyber incidents.

The Consortium is coordinated by EVIDEN TECHNOLOGIES SRL - Romania, having as partners: Engineering – Ingegneria Informatica Spa – Italy; Synelixis Lyseis Pliroforikis Automatismou & Tilepikoinonion Anonimi Etairia – Greece; SBT Poslovne Resitve Doo – Slovenia; Erevnitiko Panepistimiako Institouto Systimaton Epikoinonion Kai Ypologiston – Greece; Institut Za Korporativne Varnostne Studije Ljubljana – Slovenia; Agencija Za Komunikacijska Omrezja in Storitve Republike Slovenije – Slovenia; Urad Vlade Republike Slovenije Za Informacijsko Varnost – Slovenia; TELEKOM SLOVENIJE DD – Slovenia; Eles Doo Operater Kombiniranega Prenosnega In Distribucijskega Elektroenergetskega Omrezja – Slovenia; Directoratul National de Securitate Cibernetica – Romania; Ministerul Sanatatii – Romania; Directia Generala de Protectie Interna – Romania; Clinica Ginecologie dr. Muntean SRL – Romania; Regione Autonoma Friuli-Venezia Giulia – Italy; INSIEL - Informatica Per Il Sistema Degli Enti Locali S.P.A. – Italy;

Perifereiako Tameio Anaptyksis Attikis – Greece; Perifereiako Tameio Anaptyxis Perif Dytikis Ellados – Greece; Etaireia Ydreyseos Kai Apochetefseos Proteyoysis Anonimi Etaireia – Greece; TIMELEX – Belgium; Diadikasia Business Consulting Symvouloi Epicheiriseon AE – Greece; Carr Communications Limited – Ireland; Eviden Germany GMBH – Germany (Affiliated)

The consortium's solutions will be validated through cross-sector and cross-border pilot programmes in four EU Member States – Romania, Slovenia, Italy, and Greece, ensuring their effective implementation and harmonization across different national contexts. By facilitating collaboration between stakeholders and aligning efforts with the CER and NIS2 Directives, ENDURANCE is positioned to play a key role in securing Europe's infrastructures against a rapidly evolving threat landscape. ENDURANCE project's mission undertakes targeted activities related to:

(a) Enhance strategic cooperation and collaboration among the European CI stakeholders at all levels (bringing together 100+ relevant practitioners and experts across Europe);

(b) Develop datasets, registries, methodologies, technologies, and services (at TRL6-7) for secure sharing and federated processing of CER-relevant data, joint assessment of relevant risks and resilience, and large-scale stress-testing of preparedness;

(c) Provide harmonised and pragmatic strategy for the continuity of the interconnected essential services (adopted by 20+ relevant European sectorial and national CI authorities).

Specific objectives of the project refer to:

Objective #1 – UNITY: Encourage, enhance, and support the all-level, pan-European strategic cooperation, operational collaboration, and continuous communication, enabling exchange of experience and best practices. We will organize 12 national and 3 European workshops with competent authorities from different EU Member States (MSs), CI operators, and other relevant CI stakeholders to establish a framework for understanding the current functioning of the European CI and provide cooperation mechanisms at different levels: local, regional, national, cross-border; within and across sectors; between public and

private entities; with governments and policy makers. The necessary data will be collected for the development and co-creation of ENDURANCE results. The workshops will be gradually transformed into the Working Group on Disruption Resilience (WGDR) with the aim of having more than 100 members by the end of the project.

Objective #2 – PREPAREDNESS WITH SERVICES: Establish a trusted data space for CER-relevant data and deliver user-friendly and interoperable services for (1) secure exchange and federated processing of such data, (2) essential-service-oriented digital twins, (3) continuous identification and assessment of risks and resilience, and (4) human-centric simulation and interactive training, empowering a broader community of CI stakeholders.

Objective #3 – PREPAREDNESS WITH STRATEGY: Align and improve current practices, policies, strategies, and business continuity plans by generating a harmonized Pan-European strategy for disruption resilience. This will include a) ordinary interpretation of CER definitions; b) harmonized methodologies for cross-x risk assessments and resilience for all hazards; c) guidelines for a coordinated and effective cross-x response to disruptions; d) new models for coordinated crisis communication in situations with societal impact (pandemic, political conflicts, economic crises, natural disasters, etc.)

Objective #4 – RESOLVE THROUGH TEST: Design and coordinate large-scale and cross-x exercises with CI authorities and operators to stress test their preparedness and ensure that our results are effective and pragmatic. These will be run within 5 strategic and operational pilots (4 countries, including Romania – MESO Pilot Disruption Resilience for Digital & Health – where intersectoral challenges at local, regional and national levels will be identified, analysed and addressed).

Objective #5 – PROMOTE: Promote the ENDURANCE mission, activities, and results to the relevant CI stakeholders across Europe and generate great positive, direct, tangible, and immediate impacts.

All project outcomes will be co-created and evaluated in relevant settings with a variety of CI authorities and operators from different EU Member States, thereby preparing the results for a real-world uptake across different critical sectors and countries.

"The CRA-AI project will build highly automated AI enabled software to support SMEs and Micro SMEs on every step of their journey to achieve compliance with the Cyber Resilience Act"

Grant Agreement No. 101190243 (January 2025 - December 2026)

The Romanian National Cyber Security Directorate (DNSC) is the beneficiary of a non-reimbursable financing for the implementation of **the CRA-AI project will build highly automated AI enabled software to support SMEs and Micro SMEs on every step of their journey to achieve compliance with the Cyber Resilience Act**, acronym CRA-AI project, under the grant agreement no. 101190243. The project is financed by the granting authority: European Cybersecurity Industrial, Technology and Research Competence Centre through the Digital Europe Programme, under the call DIGITAL-ECCC-2024-DEPLOY-CYBER-06-COMPLIANCECRA topic, type of action: DIGITAL JU SME Support Actions.

The digital transformation of businesses across Europe has made cybersecurity a fundamental concern. For small and medium-sized enterprises (SMEs) and micro-enterprises, achieving compliance with the Cyber Resilience Act (CRA)[4] can be particularly challenging. Addressing this need, the CRA-AI project is set to provide an AI-driven, highly automated software platform that will simplify their compliance journey and enhance cybersecurity resilience across the European market.

The Cyber Resilience Act is a cornerstone of the EU Cybersecurity Strategy[5], introducing a CE Mark for cybersecurity compliance. Manufacturers and service providers must demonstrate that their digital products adhere to strict security standards. However, as highlighted in

[4] See details on https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.
[5] See details on https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018.

the EU Commission Impact Assessment[6], compliance is a major challenge for many SMEs, due to limited resources and expertise. The CRA-AI project aims to bridge this gap by integrating automation and AI-driven tools to facilitate compliance efficiently and cost-effectively.

This project brings together leading cybersecurity institutions and technology partners across Europe, ensuring a robust and scalable solution. The consortium is coordinated by Cyber Cert Labs LTD (Ireland), having as partners: UAB NRD CS (Lithuania), 42SECURE (Belgium), Grit Solutions Sociedad Limitada (Spain), Directoratul National de Securitate Cibernetica (Romania), Protostars AI Software Limited (Ireland), Red Alert Labs (France). The project benefits from expertise of associate partnerships with: Munster Technological University (Ireland), National Cyber Security Centre (Ireland), and Ministerie Van Economische Zaken En Klimaat (The Netherlands).

The main objective of the CRA-AI project is to develop a user-friendly AI-powered platform that will guide SMEs through every step of their compliance journey. The platform will integrate four existing cybersecurity tools and introduce new AI-based automation features to reduce complexity and costs. The key functionalities of the platform include:

- Product Inventory: Establishing an inventory of all products, components and/or modules a product or software relies on including where required a Software Bill of Materials (SBOM). This will allow the user to define a Target of Evaluation (ToE) which will define the scope of the CRA assessment.
- Risk Assessment: Performing risk assessments on the product or software to determine how its users could be impacted by vulnerabilities. Establishing the protection profile of the product or service which will define the security controls required and alignment with the essential requirements in Annex 1. Threat Modelling and Analysis (TMA) will also be included in the software

[6] See details on https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment.

to clearly identify threats and potential vulnerabilities in the product or service.

- Testing: Based on the ToE and the documented protection profile the user can define a full set of test criteria for the product or service. This can include penetration testing, vulnerability management and secure code reviews.
- Documentation: Generating the required "Information and instructions to the user" as defined in Annex 2 of the CRA. This includes contact information for the manufacturer or distributor, details of the intended use and a user-friendly explanation of the protection profile and the security controls that support the protection profile.
- Assessment: The software will align to the EUCC scheme and any associated standards that are defined by the scheme. There are two forms of assessment, self-assessment, and conformity assessment. The software will prepare and generate all the documentation related to the definition of the ToE, the protection profiles, all tests executed by or on behalf of the manufacturer or distributor and any other relevant information. This is an important activity as a manufacturer or distributor can be asked for this by a surveillance authority at any time. Also, where a conformity assessment is required, this documentation provides the Conformity Assessment Body (CAB) with all the necessary information to assess the product or service.
- Monitoring: Providing the capability to monitor the product or service for any vulnerabilities that are discovered after the product or service has been placed on the market.
- Vulnerability Disclosure: When vulnerabilities or flaws are discovered in a product or piece of software, other software or product vendors who have relied on or embedded this as a component in their product need to be alerted so they can take appropriate action.

To maximize its impact, the CRA-AI project is structured into seven work packages: Project Management and Coordination, Dissemination, Product development – CRA workflow, Product

development – Vulnerability management, Product development – Secure code analysis, Product development – Human security, Pilot cases. By combining AI-driven automation with an intuitive, easy-to-use platform, the CRA-AI project will significantly lower compliance costs and streamline regulatory processes for SMEs. This will empower small businesses to meet cybersecurity requirements efficiently, ultimately strengthening the EU's digital resilience.

The Romanian National Cyber Security Directorate is the leader of the dissemination activities, using the "Cyber Cert Labs Readiness Assessment" survey as part of a market scan for SMEs in Romania. The output of this market scan will help inform the product designers, produce a national level report on CRA readiness for SMEs, and link with other National Coordination Centres (NCCs). Based on the market scan, the workshops, webinars and the national event organised by DNSC will document a case study which will be available to the NCCs working groups, to raise awareness on the Cyber Resilience Act fo for SMEs[7].

[7] We thank PhD Claudia Lascateu for the presentation.

CALL FOR PAPERS *ROMANIAN INTELLIGENCE STUDIES REVIEW*

"Mihai Viteazul" National Intelligence Academy publishes the *Romanian Intelligence Studies Review* (RISR), a high-quality peer reviewed and indexed research journal, edited in English and Romanian twice a year.

The aim of the journal is to create a framework for debate and to provide a platform accessible to researchers, academicians, professional, practitioners and PhD students to share knowledge in the form of high quality empirical and theoretical original research papers, case studies, conceptual framework, analytical and simulation models, literature reviews and book review within security and intelligence studies and convergent scientific areas.

Topics of interest include but are not limited to:

- Intelligence in the 21st century
- Intelligence Analysis
- Cyber Intelligence
- Open Source Intelligence (OSINT)
- History and memory in Intelligence
- Security paradigms in the 21st century
- International security environment
- Security strategies and policies
- Security Culture and public diplomacy

Review Process: RISR shall not accept or publish manuscripts without prior peer review. Material which has been previously copyrighted, published, or accepted for publication will not be considered for publication in the journal. There shall be a review process of manuscripts by one or more independent referees who are conversant in the pertinent subject area. Articles will be selected based on their relevance to the journal's theme, originality and scientific correctness, as well as observance of the publication's norms. The

editor evaluates the recommendation and notifies the author of the manuscript status.

The review process takes maximum three weeks, the acceptance or rejects notification being transmitted via email within five weeks from the date of manuscript submission.

Date of Publishing: RISR is inviting papers for No. 35 and 36 and which is scheduled to be published on June and December, 2026.

Submission deadlines: February 1st and July 1st

Author Guidelines: Author(s) should follow the latest edition of APA style in referencing. Please visit www.apastyle.org to learn more about APA style, and http://www.animv.ro for author guidelines. For more details please access the official website: **animv.ro** and **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