RESILIENCE OF INTELLIGENCE SERVICES IN THE ERA OF HYBRID WARFARE

Dr. Răzvan CURCULESCU

Resilience Core Initiative Association-Thor member, Bucharest

DOI: 10.55535/RMT.2025.3.24

This article provides an exhaustive examination of the operational and institutional resilience of intelligence services in NATO and EU countries in the context of the hybrid war waged by the Russian Federation, as well as the clarification and delimitation of the concept of resilience, as reflected in the programmatic documents of organizations relevant in the field of security, analyzing the measures that can contribute to increasing the resilience of intelligence services, by correlating them to the effects of hybrid warfare on all dimensions of democratic society.

In a period deeply marked by the growth of disinformation, the diversification of cyber-attacks and the increase in the dynamics of influence actions led by state actors, a doctrinal and institutional reset is necessary, as well as the consolidation of cooperation at the level of partner services, through a comparative analysis of public, security policies and strategic documents, highlighting the conceptual and operational differences of NATO and EU states, but also the elements of convergence in the field of resilience from the perspective of designing an integrated intelligence architecture.

Keywords: hybrid warfare; resilience; intelligence services; NATO; EU;

CONCEPTUAL APPROACHES – FROM HYBRID WARFARE TO RESILIENCE

The concept of *hybrid warfare*, enunciated and analyzed by Hoffman in 2007, designated an activity aimed at identifying and exploiting the systemic vulnerabilities of a state considered a target, through actions and operations that do not represent a direct confrontation. In the current period, we observe that hybrid warfare has become part of the strategic confrontation between powers, manifesting itself through the combination of conventional and unconventional means (Hoffman, 2007, p. 8), such as cyber, informational, energy, economic and more.

If hybrid warfare was initially linked to the 2006 Lebanon conflict, in the last decade it has been observed that the **Russian Federation** combines conventional and unconventional means, military and non-military, in a coordinated campaign aimed at achieving political and military objectives, in a first stage, without declaring an open war. Through instruments such as: cyber operations, disinformation campaigns, economic or energy pressures, the use of proxy actors (militia, mercenaries, criminal organizations), political and psychological interventions, sabotage, drone incursions, its aim is to divide and weaken the adversary's decision-making capacity, without a classic confrontation (Mumford, 2020, pp. 3-4; Galeotti, 2016, pp. 5-9).

Hybrid warfare exploits the modern *"fog of war"* (Mumford, 2020, p. 5). Hybrid actors, state or non-state, simultaneously launch massive flows of contradictory information (fake news, fabricated sources, manipulated data), designed to saturate the analytical capacity of the adversary, and the examples below, which present real examples that can be classified as this type of war, highlight the difficulty of countering such actions.

a. **Erosion of information certainty** – in the hybrid war waged/carried out by the Russian Federation, truth has become a battlefield. The Russians use **disinformation, deepfakes, source manipulation and controlled leaks** to pollute the information environment. The aim is twofold: to **divert the internal analysis** of the intelligence structures of the targeted countries and to **undermine the trust of decision-makers** in their own information apparatus. Thus, during the conflict in Ukraine (2022-2024), Russia simultaneously launched contradictory narratives *("there is no invasion"/*

"liberation operation"), generating confusion including in OSINT flows. Western services countered Russian attacks on this dimension **through multi-domain fusion and collaborative analysis NATO-EU-Ukraine** (NATO StratCom COE, 2023).

b. **Increasing pressure on cyber infrastructure (technological resilience)** – hybrid warfare includes attacks on the **IT infrastructure of intelligence services** – classified servers, encrypted channels, operational databases or SCADA systems.These attacks are intended to **temporarily *"blind"* the capacity for analysis and response**. In 2021, attacks on government networks in Ukraine and Poland (the *"Ghostwriter"* and *"Sandworm"* campaigns) demonstrated how an adversary can temporarily paralyze strategic intelligence communication. NATO and the EU have provided joint support through the CCDCOE and Hybrid CoE, testing crisis response (ENISA, 2022).

c. **Human and organizational overstrain (organizational resilience) – hybrid warfare implies continuous activity, permanent uncertainty and media pressure**. Intelligence services, accustomed to linear information cycles, must now operate in a constant alert mode.After 2014, the Baltic services (Estonia, Latvia, Lithuania) introduced continuous training programs in psychological resilience for intelligence analysts, precisely to counteract the effects of Russian information warfare (Hybrid CoE, 2021).

d. **Threat to public credibility (societal resilience)** – hybrid adversaries not only attack information networks, but also **the public image of intelligence institutions**, with the aim of losing public trust and isolating the services from their own government. In disinformation campaigns in Central Europe (2018-2022), the services were direct targets: false accusations of domestic espionage or corruption aimed at weakening public trust.The Nordic countries countered through strategic communication resilience programs coordinated with NATO StratCom COE (Riga).

e. **Changing the defense paradigm (systemic resilience)** – hybrid warfare forces the transition from the classic paradigm – *"intelligence reacts to threats"* – to a proactive and integrated one: *"intelligence prevents and shapes the security environment".* The NATO JISR (Joint Intelligence, Surveillance and Reconnaissance) model and the EU-SIAC partnership are concrete examples of **integrated systemic resilience**, which ensures information continuity even in the event of the degradation of an intelligence node (NATO, 2020; EEAS, 2022).

Based on the examples above, it is clear that hybrid warfare forces intelligence services to become **living and adaptive organisms**, capable of operating in ambiguity and continuous pressure. Their resilience no longer depends solely on technology or secrets, but on the **balance between people, information and trust**. In the hybrid era, the strongest intelligence service is not the one that knows the most, but the one that **resists uncertainty the best** (Hybrid CoE, 2023, pp. 4-6; Linkov, Kott, 2019, pp. 3-5).

Thus, we can say that hybrid warfare acts as a **permanent stress test** for intelligence services, forcing them to rethink their mission, structure and internal culture, while resilience no longer means just survival after an attack, but also the **ability to function effectively in continuous uncertainty**.

Against the backdrop of hybrid warfare, intelligence services have become the main institutions that contribute to strengthening the resilience of target states, pillars of strategic resilience, by carrying out early warning and decision-making protection missions.

Conceptually, we will define resilience as the capacity of a system to absorb shocks and maintain its essential functions in crisis situations. Adapting the concept to the subject of this research, we can consider that the resilience of intelligence services represents the state in which they are operationally, organizationally and cognitively adapted to deal with crisis situations generated by hybrid warfare.

In the specialized literature we find the concept of resilience treated from different perspectives – *societal resilience* (Chandler, 2014, p. 56), *technological resilience* (Linkov, Trump, 2019, pp. 9-34), but that of *state resilience*, strategic or punctual resilience, of intelligence services, is a field in which this concept is relatively new. An important point in its definition is the moment of the illegal annexation of the Crimean Peninsula by the Russian Federation (2014), which led NATO and the EU to conceptualize the notion of resilience at the level of the two international organizations.

In 2022, NATO (NATO, 2022) and, subsequently, the EU in 2023 (ENISA, 2023), launched a series of policies aimed at strengthening the resilience of states against the threats of hybrid warfare, highlighting cyber threats and information aggression as high-risk factors affecting the security of member states. In that context, we can see the establishment of the principle that the resilience of intelligence services was directly influenced by the adaptation of operational capabilities to this new type of threats. We withhold here the reference framework established by NATO by defining the *"seven basic requirements for resilience"* (NATO, 2016, para. 73), but also the mechanisms established by the EU through the Hybrid Fusion Cell (European Commission & High Representative, 2016, Hybrid Fusion Cell section) and the Cybersecurity Strategy (European Commission, 2020).

The comparative analysis of how the two organizations approach the concept of resilience will highlight elements of divergence and convergence, but will emphasize that the resilience of Western intelligence services will not be achievable in the absence of deep cooperation.

The study of data from the public space reveals that the term resilience has a complex meaning. Starting from the theoretical approach that shows that a system, whatever it may be, is resilient if it has the capacity to maintain its basic functions in the event of crises, we observe that in the case of intelligence services these crises, which we can also call disruptions, can be related to terrorism, espionage, cyber-attacks, energy and even economic crises.

We note that in the field of security and, especially in the area of intelligence, the concept of resilience will include as main actors the states, with all their component elements that need to be defended, regardless of the type of threats generated by hybrid warfare. In other words, the resilience of intelligence services becomes a guarantor of the ability of states to manage threats and recover their basic functionalities in the event of security incidents. In this way, states will succeed in maintaining social and political stability, necessary for economic development and maintaining the rule of law.

Against this background, the resilience of intelligence services will be given by their ability to anticipate threats and to adapt proportionate measures in order to protect democratic values, critical infrastructures and public policies. Anticipation is one of the most difficult and complex missions in the intelligence area (Lowenthal, 2017, p. 148) and cannot be achieved in the absence of an increase in the capacity to obtain information, including through cooperation, but especially by increasing their strategic analysis capacity. Experience has shown that the adaptation of intelligence services is given, first of all, by the ability of these structures to learn quickly and efficiently from their own activity but also from the experience of partners.

Therefore, starting from the general interpretation of resilience, we can consider that the resilience of an intelligence service represents the ability to anticipate, manage, counteract and recover from a crisis (disruption).To support the argument, disruption will be understood as any direct or indirect action that was not anticipated, such as: information leaks, cyber-attacks, political pressures, information manipulation or major dysfunction (economic, political, social, military).

Based on these conceptual approaches, in the context of threats specific to hybrid warfare, the characteristic elements of the resilience of intelligence services in the Euro-Atlantic space can be detailed, by grouping them by dimensions, as follows:

❖ **Organizational** resilience (Lengnick-Hall, Beck, Lengnick-Hall, 2011, p. 244), as the manner in which intelligence services manage, through the practice of modern management and an organizational culture based on leadership, to quickly adapt the organization to operational changes that may cause disruptions in the specific activity. Optimal organizational adaptation to technological and geopolitical changes generated by hybrid warfare will be a key factor in maintaining the trust and morale of those who work in this field, in order to fulfill the missions of the services of which they are part.

❖ **Informational** resilience (Wardle, Derakhshan, 2017, p. 16) – is represented by the increase in the quality of information obtained and the superior capacity for analysis and integration of these in order to be able to recognize and counter attacks against intelligence services. In general, attacks can be of the type of fake news or disinformation regarding the role and place of a service in a democratic state. Although very rare in the Euro-Atlantic space, there have been situations in which certain individuals have betrayed the interests of some services and, implicitly, of the states of origin. Against this background, informational resilience will be achieved in the situation in which intelligence services will adapt internal rules in such a way as to prevent possible infiltrations, leaks of information, double sources or even betrayals.

If the two dimensions are very much related to the intrinsic capacity of intelligence services to be resilient and most of the time the listed aspects are less known to the general public, the following dimensions of intelligence services' resilience are usually visible and likely to seriously affect the security of the states they are part of and implicitly the security of the Euro-Atlantic space.

❖ **Operational** resilience (Duchek, 2020, p. 215) of intelligence services is given by the permanent capacity to obtain, analyze and exploit strategic information even when there are crisis situations. Hybrid warfare will constantly generate new, sometimes unforeseen, situations by capitalizing on new innovative technologies, while exploiting vulnerabilities. We are considering here a possible cyber-attack or an act of sabotage on critical infrastructures.

❖ **Societal** resilience refers to the capacity of a society to absorb major shocks (natural disasters, pandemics, economic crises, etc.), to adapt and recover from the shock (Chandler, 2014, p. 56), so we will consider that, in a democratic state, an intelligence service will have an important place in the societal dimension, as an integral part of society, with a well-defined role of defending the population, strategic decisions, and critical infrastructures against the new challenges generated by hybrid warfare.

❖ **Strategic** resilience (Hamel, Välikangas, 2003, p. 52) is, in the author's opinion, the most important dimension of an intelligence service in the event of major disruptive factors such as those specific to hybrid warfare. The role of an intelligence service in maintaining the decision-making capacity of a state in times of major crisis (war or severe damage to critical infrastructure) is essential in a democratic state.

THE RESILIENCE OF INTELLIGENCE SERVICES IN EURO-ATLANTIC STRUCTURES

To better understand the field, we will conduct a comparative analysis of how resilience is approached at NATO and EU levels, while also presenting a series of considerations regarding how Romania approaches this field.

The North Atlantic Treaty Organization/NATO is a political-military alliance formed in 1949 with the primary purpose of ensuring the collective defense of its member states. NATO is *"a political and military alliance of countries in Europe and North America, the purpose of which is to guarantee the freedom and security of its members by political and military means"* (NATO, What is NATO?).

The European Union/EU is a political and economic union of 27 European states that have decided to cooperate closely to ensure peace, stability and prosperity on the continent. The EU's main role is to facilitate cooperation between member states so that they are stronger together than apart, maintaining peace and supporting economic and social development (EU, What is the European Union?).

Given the very definitions of the two organizations, it can be deduced that resilience is also approached on the specifics of each organization, but the policies and strategies adopted converge towards the same objective, namely, increasing resilience. Both organizations, NATO and the EU, have developed a mix of policies and strategies through which the resilience of intelligence services is built, but also common structures dedicated to integrated analysis, the conduct of joint exercises and the improvement of the legislative framework necessary to strengthen cooperation. Thus, we can say that an effect of the threats of hybrid warfare is also the strengthening of political-military cooperation with civil society to increase societal resilience, especially to cyber-attacks and disinformation.

RESILIENCE OF INTELLIGENCE SERVICES IN NATO

From studying the organization's planning and leadership documents (NATO, Resilience Committee, 2022), it is found that NATO considers **resilience to be the key element** in its policy of deterring hybrid warfare threats, by permanently requesting allies to permanently take the necessary measures to ensure operational capabilities in crisis situations. According to NATO, *"national and collective resilience capacity is an essential basis for the credibility of deterrence"* (NATO, 2024).

NATO initiated, supported and developed the concept of joint deterrence capabilities and supported the establishment of **integrated analysis structures**, such as the Joint Intelligence and Security Division (JISR) and the NATO Intelligence Fusion Centre (NIFC) (NATO, 2024).In particular, the work of these structures has increased the exchange of information between Allies and, consequently, has contributed to increasing the quality of operational decisions. For example, the NIFC *"provides SACEUR (Supreme Allied Commander Europe) with relevant, accurate and timely information to support the planning and execution of operations"* (NATO Intelligence Fusion Centre, *"Mission"* section).

In the field of cyber defense, NATO has launched a series of **joint exercises** through which partner states can train their specialists by participating in such formats. For example, through the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Tallinn, NATO creates realistic defense scenarios that increase the resilience of intelligence services in the context in which they have become increasingly dependent on digital infrastructures. Through these joint exercises, intelligence services have developed the capacity for interoperability and adequate response to threats specific to hybrid warfare.

In essence, NATO's defense doctrine considers military resilience to include the civil and commercial readiness that the military force needs to deploy troops rapidly and freely throughout the Alliance (NATO, 2022, section on *"layered resilience"*). A final aspect that we consider in analyzing the increase in intelligence resilience is the fact that NATO has pursued and succeeded in **unitary standardization of communication** at the Alliance level.

Through instruments such as ***Joint Intelligence, Surveillance and Reconnaissance (JISR)*** *– an integrated framework in the military field that combines intelligence, surveillance and reconnaissance capabilities to support strategic and operational decisions* and ***Federated Mission Networking (FMN)*** – which is a NATO initiative aimed at the rapid and interoperable creation of mission networks for allied and partner forces in joint operations, NATO has reduced the risk of *"single points of failure"* in joint operations.

As a conclusion of how resilience contributes to collective defense, we mention the Allied Joint Doctrine in the Allied Joint Publication (AJP) which emphasizes that *"the formation of combined power ... requires layered resilience in the context of defense."* (NATO, 2022, p. 73).

RESILIENCE OF EU MEMBER STATES' INTELLIGENCE SERVICES

In the context of the intensification of hybrid threats generated by the actions of the Russian Federation, especially cyber, but also of a security environment with a rapid dynamic of evolution and, implicitly, a change in the strategic environment, the EU has adopted a series of political and normative instruments with the aim of strengthening its strategic resilience with a direct impact on strengthening the resilience of intelligence services.

To provide greater clarity on this topic, in this article we will review the key elements of EU measures that contribute to the strategic and operational resilience of intelligence services in EU Member States, such as: Strategic Compass and Single Intelligence Analysis Capacity (SIAC); tools against hybrid threats; cyber regulations and standards; practical cooperation and joint capabilities.

a. **Strategic Compass & SIAC (Single Intelligence Analysis Capacity)**. The Strategic Compass is the EU's strategic guidance document in the field of security and defence, adopted by the Council of the European Union in March 2022, which sets out concrete objectives by 2030 to strengthen resilience, through measures to increase European capacities for anticipation, risk assessment and crisis management. The Strategic Compass is built on four pillars *("Act", "Invest", "Partner"* and *"Secure")* and includes measures to anticipate, deter and respond to threats. (Council of the EU, 2022).

In this context, SIAC, which includes EU INTCEN (the civilian intelligence component) and EUMS-INT (the military component within the EU General Staff), was designed as a single point for integrated strategic analysis, with a central role in providing knowledge (Blockmans, Crosson, Paikin, 2022 pp. 4-6).

Its structuring as a *"single entry point"* for strategic analysis provided by member states has allowed the integration of civil and military intelligence flows with the aim of increasing the quality of common analytical products. The introduction of this mechanism has resulted in increased coherence of strategic decisions at the level of EU decision-makers and a clearer overview of hybrid warfare threats. Against this background, the EU has strengthened its strategic resilience for managing complex crises.

b. **Cyber regulations and standards**. NIS2 and the role of ENISA – the new NIS2 (Network and Information Security Directive) is the EU's fundamental legal framework for ensuring a high common level of cybersecurity in essential sectors. It represents the most comprehensive European legislative framework for protecting critical infrastructures and extends security requirements to several sectors — energy, transport, health, public administration, telecommunications, finance, digital service providers, etc. (EU, Directive 2022/2555).

The main effects of NIS2 on resilience include: clear obligations to prevent, detect and promptly report cyber incidents; governance and risk management requirements at the level of the management of organizations; minimum standards for network and supply chain security; more severe sanctions for non-compliance. Thus, this Directive introduced strict elements regarding risk management, incident reporting and cross-border cooperation.

The European Union Agency for Cybersecurity (ENISA) plays a central role in the knowledge and implementation of cyber directives. With an extensive role in the implementation of binding EU legislation, ENISA provides: technical guidance and best practices, coordination of responses between Member States, threat assessments (Threat Landscape Reports), support for testing and auditing of critical infrastructures.(EU, 2019, art. 8–11).

Together, NIS2 and ENISA raise the overall level of **cyber hygiene** reduce structural vulnerabilities and narrow the attack surface exploitable by adversaries – essential for the resilience of intelligence services, their digital infrastructures, critical infrastructures and, ultimately, of Member States (EU-ENISA, 2023, pp. 6-7).

c. **Tools against hybrid threats**. In cooperation with NATO, the EU has created the *European Centre of Excellence for Countering Hybrid Threats* (Hybrid CoE), which is the main platform for cooperation in the joint management of hybrid threats (European Commission& High Representative, 2016, *Hybrid Threats Section*).The Centre functions as a hub of expertise for the identification, analysis and responses to hybrid threats, in areas such as: disinformation and manipulation campaigns, foreign political interference, information warfare, economic and energy pressures, the combination of cyber operations and physical actions (sabotage, border provocations, etc.).

Hybrid CoE not only produces complex analyses and scenarios, but also organizes multilateral exercises, applied training and joint projects. In this way, the center strengthens societal resilience and sectoral response capacity, in the following directions:

- increases the capacity of institutions to recognize and counter interference;
- provides tools for a coordinated response between sectors (government, infrastructure, private sector);
- contributes to the synchronization of measures between the EU, NATO and participating states.

d. **Practical cooperation and joint capabilities**. In addition to institutional and normative frameworks, the EU has also invested in operational tools that contribute to interoperability between intelligence services. These tools play a major role in increasing the resilience of these services in managing the Russian Federation's hybrid threats. In this dimension, the following elements are relevant:

- **Space and satellite capabilities** (e.g. Galileo, Copernicus), which provide secure communications, advanced imaging and monitoring of critical environments.
- **Geospatial imaging and analysis centres**, which support the **Common Security and Defence Policy** (CSDP) and crisis response.
- **Permanent Structured Cooperation** (PESCO) initiative, aimed at creating joint capabilities (e.g. medical commands for maritime surveillance, secure communication networks).
- **CSDP projects** including joint training, information sharing and the development of crisis management tools.

In conclusion, through the above, the EU has managed to design an architecture aimed at strengthening the resilience of states and implicitly of intelligence services, these mechanisms being likely to strengthen the resilience of the EU as a whole by creating an integrated security environment, capable of generating adequate reactions to the continuously evolving threats generated by the Russian Federation.

ROMANIA'S OPTIONS AS A NATO AND THE EU MEMBER

Since 2014, in the context of the illegal annexation of the Crimean Peninsula, Romania has initiated a broad process of **doctrinal alignment** with NATO and EU standards, reflected in the *National Defense Strategy (2020-2024)* and in internal reforms of the intelligence services. Based on these, **national resilience** can be understood as the **capacity of state institutions, the economy and society to protect essential functions, to prevent and manage major disruptions and**

to quickly return to a state of normality, in line with the *"extended national security"* approach defined in the National Defense Strategy (Presidential Administration, 2020, pp. 7-8).

In addition to these guidelines, the key institutions involved in the implementation of security, intelligence and resilience policies in Romania are also indicated:

❖ **The Romanian Intelligence Service (SRI)** is the main domestic intelligence service of Romania and acts as the *national authority* in the field of cybersecurity. In this role, the SRI coordinates **cyber resilience** policies, manages the protection of critical infrastructures of national interest and ensures the prevention, detection and counteraction of cyber and terrorist threats. Through the National Cyberint Center and through cooperation with the National Directorate of Cyber Security/ DNSC, the SRI contributes to strengthening national incident response capabilities and counters complex cyber-attacks (Ib., pp. 26-27, 34).

❖ **The Foreign Intelligence Service (SIE)** is responsible for collecting, analyzing and providing decision-makers with information on **external risks and threats** to Romania. In the context of national resilience, SIE monitors geopolitical developments, international crises, hybrid risks, cyberattacks originating from outside the country, as well as hostile actors. SIE also coordinates international cooperation with partner services, organizations such as NATO and the EU, and facilitates the exchange of strategic information relevant to national security, the service being responsible for assessing external risks and international cooperation. Against the backdrop of hybrid warfare, the SIE has intensified cooperation with EU structures, participating in the analytical flows of **INTCEN** and the **Hybrid Fusion Cell** (Foreign Intelligence Service, n.d., Mission and international cooperation).

❖ **The Supreme Council of National Defense (CSAT)** represents the **strategic level of integration** of security, defense and intelligence policies. The Council approves national strategies (e.g.: National Defense Strategy, Cyber Security Strategy, etc.), establishes priorities in the information-operational field, coordinates the activity of intelligence institutions and validates the necessary measures to strengthen national resilience. CSAT functions as a unified decision-making platform between the President of Romania, the Government and the structures with responsibilities in the field, functioning as a strategic integrator of intelligence and resilience policies.

Romania began to develop, after 2020, a **cognitive resilience component**, focused on strategic education and combating disinformation. Campaigns such as #SiguranțaOnline (DNSC, 2022) and university programs in *cyber diplomacy* and *strategic analysis* contribute to the formation of a *"culture of resilience"* in the public space.

In cooperation with StratCom COE, Romania implemented strategic communication exercises and information crisis management simulations, including disinformation scenarios during elections. This societal dimension complements the technological resilience architecture, bringing to the forefront the idea of **cognitive security** – defending the collective ability to distinguish truth from manipulation (Waltzman, 2017, p. 2).

Although Romania has made significant progress, in the author's opinion, a number of structural vulnerabilities persist: institutional fragmentation between SRI, SIE and other government agencies; shortage of personnel specialized in data analysis and digital intelligence; technological dependence on external providers in the government IT infrastructure; still rigid legislation on data exchange between institutions. However, these challenges are partially offset by international cooperation and the continuous process of institutional learning.

The comparative analysis of the way Romania approaches the concept of resilience in relation to NATO and the EU, highlighted the fact that our country is positioned in an area of **doctrinal convergence** between the two Euro-Atlantic organizations. This strategic positioning is not only a consequence of dual membership, but the result of a **deliberate policy of institutional adaptation**. In the author's opinion, in the last ten years, the intelligence services in Romania have moved from a defensive paradigm, focused on information protection, to a proactive one, based on **anticipation, sharing and adaptability**.

Through constant cooperation with **NATO centers of excellence (CCDCOE, StratCom COE)** and participation in European analysis mechanisms (INTCEN, Hybrid Fusion Cell), Romania has developed a multiple resilience, combining military, civilian and cognitive capabilities, so that Romania is described in the specialized literature as an *"emerging cybersecurity hub"* in Eastern Europe (Popescu, 2022). However, this positioning also brings vulnerabilities, especially since the geographical proximity to conflict areas (Black Sea, Ukraine, Republic of Moldova) amplifies the pressure on the intelligence structures in our country.

In the field of intelligence, **cognitive resilience** refers to the ability of analysts and decision-makers to recognize, interpret and react to manipulative information. This is closely linked to **institutional resilience**, which involves flexible structures and rapid information flows. Out of the need to deal as effectively as possible with the current challenges it faces, Romania has begun to integrate these two levels through interdisciplinary training programs, such as:

- *strategic intelligence and decision-making analysis* courses organized at the *"Mihai Viteazul"* National Intelligence Academy;
- SRI–MAE–DNSC cooperation for training personnel in the field of cyber diplomacy;
- partnerships with civilian universities for disinformation research (University of Bucharest, SNSPA, *"Babeș-Bolyai"* University).

This approach, in which the analysis process is doubled by an internal mechanism of self-correction and institutional learning, inspired by complex systems theory (Chandler, 2014), provides flexibility in managing uncertainty and reduces the risk of cognitive errors in the strategic decision-making process.

In conclusion, given the above, at a theoretical level, Romania assimilates models of increasing the resilience of intelligence services in the Euro-Atlantic space, where NATO provides the strategic defense framework and the EU provides the governance and civil cooperation architecture. Overall, Romanian intelligence services are **evolving from reactive security to resilience**, having a solid foundation in the ability to learn and adapt to the security context generated by the hybrid war led by the Russian Federation (Manea, 2021, pp. 52-53).

CONCLUSIONS

The analysis carried out in this scientific article confirms that the **resilience of intelligence services** represents an essential component of the 21st century security architecture, especially in the context of hybrid warfare.

Essentially, **NATO** focuses on interoperability, joint military capabilities and collective exercises, while the **EU** promotes strategic coordination, cyber regulation and societal resilience. NATO and the EU, although starting from distinct institutional paradigms, have converged towards a **common vision**: protecting democratic societies through an intelligence system capable of anticipating, absorbing and adapting to complex shocks. One of the most sensitive issues of intelligence resilience is the **balance between transparency and security**, so while the EU promotes a culture of open governance, NATO and national intelligence structures traditionally operate within a narrow, confidential framework.

To the extent that elements such as trust versus sharing (sometimes certain rivalries limit the exchange of information);legal/constitutional limitations (given by the sovereignty of states);dependence on some private infrastructures (which sometimes do not comply with the same standards of secrecy/security) will be overcome, the resilience of intelligence services will reach an optimal level for countering hybrid threats that are becoming increasingly complex, by combining multiple types of manifestations (e.g. combining cyberattacks with disinformation).

Romania, located at the intersection of these two systems, manages to build a **mixed resilience** in the field of intelligence services, adapted to its own needs and vulnerabilities. By reforming in relation to NATO and EU standards, Romanian intelligence services have become an active part of information flows, have proven that they have the capacity to adapt institutionally and to develop strategic analysis capabilities and, implicitly, adequate operational resilience to manage the threats of the hybrid war waged by the Russian Federation against the Euro-Atlantic space.

BIBLIOGHRAPHY:

1. Administrația Prezidențială (2020). *Strategia Națională de Apărare a Țării pentru perioada 2020–2024. O Românie sigură și prosperă într-o lume marcată de noi provocări*. București, https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020.pdf, retrieved on 15 October 2025.
2. Blockmans S., Crosson D.M., Paikin Z. (2022). *CEPS Policy Insights*, https://cdn.ceps.eu/wp-content/uploads/2022/03/CEPS-PI2022-14_EU-Strategic-Compass.pdf, retrieved on 14 Octobre 2025.
3. Chandler, D. (2014). *Resilience: The Governance of Complexity*. Routledge.
4. Council of the European Union (2022). *A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security*, https://www.consilium.europa.eu/en/policies/strategic-compass/, retrieved on 12 October 2025.
5. Duchek, S. (2020). *Organizational resilience: A capability-based conceptualization*. Business Research, 13(1), pp. 215-246.
6. ENISA (2023). *ENISA Work Programme 2023. European Union Agency for Cybersecurity*. European Union, https://www.enisa.europa.eu/publications/corporate-documents/work-programme-2023, retrieved on 12 October 2025.
7. ENISA (26 June 2025). *NIS2 technical implementation guidance*. European Union Agency for Cybersecurity, https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance, retrieved on 10 October 2025.
8. European Commission & High Representative of the Union for Foreign Affairs and Security Policy (2016). J*oint framework on countering hybrid threats: A European Union response*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018, retrieved on 11 October 2025.

9. European Commission (2020). *The EU's cybersecurity strategy for the digital decade*, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade, retrieved on 10 October 2025.
10. European External Action Service (EEAS) (2022). *EU Single Intelligence Analysis Capacity (SIAC): Overview and functions*. Brussels: EEAS, https://www.eeas.europa.eu, retrieved on 11 October 2025.
11. European External Action Service (2022). EU Intelligence and Situation Centre (INTCEN): Overview and functions, https://www.eeas.europa.eu, retrieved on 10 October 2025.
12. European Union Agency for Cybersecurity (ENISA) (31 January 2023). *The NIS2 Directive: Network and information systems directive 2*, https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/raising-awareness-campaigns/network-and-information-systems-directive-2-nis2, retrieved on 10 October 2025.
13. European Union. What is the European Union?, https://op.europa.eu/webpub/com/eu-and-me/en/WHAT_IS_THE_EUROPEAN_UNION.htm, retrieved on 10 octombrie 2025).
14. Galeotti, M. (2016). *Hybrid War or Gibridnaya Voyna? Getting Russia's non-linear military challenge right*. Mayak Intelligence Report.
15. Hamel, G., Välikangas, L. (2003). *The quest for resilience*. Harvard Business Review, 81(9), pp. 52-65
16. Hoffman, F.G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies.
17. Hybrid Centre of Excellence (2021). *Building resilience against hybrid threats: Lessons learned from the Baltic region.* Helsinki: Hybrid CoE.
18. Hybrid Centre of Excellence (2023). *Hybrid influence operations and resilience*. Helsinki: Hybrid CoE.
19. Lengnick-Hall, C.A., Beck, T.E., Lengnick-Hall, M.L. (2011). *Developing a capacity for organizational resilience through strategic human resource management,* in *Human Resource Management Review*, 21(3), https://doi.org/10.1016/j.hrmr.2010.07.001, retrieved on 10 October 2025.
20. Linkov, I., Kott, A. (2019). *Fundamentals of cyber resilience: Building a secure and resilient digital society*. Springer.
21. Linkov, I., Trump, B.D. (2019). *The science and practice of resilience*. Springer.
22. Lowenthal, M.M. (2017). *Intelligence: From secrets to policy* (7th ed.). CQ Press.
23. Manea, A. (2021). *Adaptabilitatea serviciilor de informații românești în contextul amenințărilor hibride.* Analize de Securitate, 10(2), pp. 45-63.
24. Mumford, A. (2020). *Ambiguity in hybrid warfare*. Helsinki. The European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/wp-content/uploads/2020/09/202009_Strategic-Analysis24-1.pdf, retrieved on 15 October 2025.

25. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2021). Locked Shields 2021 after-action report. Tallinn: CCDCOE, retrieved on 15 October 2025.
26. NATO Intelligence Fusion Centre (n.d.). *Who we are/Mission*, https://web.ifc.bices.org.html, retrieved on 12 October 2025.
27. NATO StratCom Centre of Excellence (2023). *Resilience in the information environment: Countering hybrid narratives.* Riga: NATO StratCom COE, retrieved on 12 October 2025.
28. NATO, https://ccdcoe.org/locked-shields, retrieved on 11 October 2025.
29. NATO, https://www.act.nato.int/activities/federated-mission-networking.html, retrieved on 11 October 2025.
30. NATO, https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_(1)_2437.pdf, retrieved on 11 October 2025.
31. NATO, https://www.nato.int/en/about-us/organization/nato-structure/resilience-committee, 7 October 2022, retrieved on 11 October 2025.
32. NATO (2016). *Commitment to enhance resilience* (Warsaw Summit Communiqué, para. 73). North Atlantic Treaty Organization, https://www.nato.int, retrieved on 11 October 2025.
33. NATO (2020). *Joint Intelligence, Surveillance and Reconnaissance (JISR)*. Brussels: NATO Public Diplomacy Division, https://www.nato.int/en/what-we-do/deterrence-and-defence/joint-intelligence-surveillance-and-reconnaissance, retrieved on 11 October 2025.
34. NATO (2022), https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_(1)_2437.pdf, retrieved on 12 October 2025.
35. NATO (2022). *Resilience and defence: Strengthening NATO's deterrence and defence posture.* Brussels: NATO.
36. NATO (2024). *Resilience, civil preparedness and Article 3*, https://www.nato.int/cps/en/natohq/topics_132722.htm, retrieved on 10 October 2025.
37. North Atlantic Treaty Organization. *What is NATO?*, https://www.nato.int/en/what-is-nato.html, retrieved on 10 October 2025.
38. Popescu, A. (2022). *Evoluții recente în securitatea cibernetică din Europa Centrală și de Est*, in *Revista Română de Studii de Securitate*, 5(2), pp. 45-60.
39. Rathje, S., Navarre, A. (2022). *What Is Societal Resilience?,* AXA Research Fund.
40. Serviciul de Informații Externe (n.d.). *Misiune și cooperare internațională*, https://www.sie.ro/, retrieved on 12 October 2025.
41. Serviciul Român de Informații (2023). *Raport de activitate 2022-2023*. București.
42. UE (2019). *Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act).*

Official Journal of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881, retrieved on 12 October 2025.

43. Waltzman, R. (2017). *The weaponization of information: The need for cognitive security* (Testimony before the U.S. Senate Armed Services Committee). RAND Corporation, https://www.rand.org/pubs/testimonies/CT473.html, retrieved on 12 October 2025.
44. Wardle, C., Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making* (p. 16). Council of Europe.