THE CONTEMPORARY SECURITY PROVISION MODEL IN THE INTELLIGENCE PRACTICE OF THE REPUBLIC OF ROMANIA

Andriy Stroev

PhD student, expert, e-mail: strilchuk7sv@gmail.com, ORCID: https://orcid.org/0009-0003-2188-4327

Ministry of Defense of Ukraine, Kyiv, Ukraine

Received: December 15, 2025 | Revised: December 28, 2025 | Accepted: December 31, 2025

UDC 351.86:327:355.40(498)

DOI: https://doi.org/10.33445/psssj.2025.6.4.5

Abstract

The article provides a comprehensive analysis of the contemporary security provision model within the intelligence practices of the Republic of Romania in the context of the evolving security environment. It examines the institutional architecture of the Romanian intelligence community, the functional specificities of its key actors, and their role in the system of strategic state governance. It is established that the Romanian model is characterised by a predominance of counterintelligence, the integration of intelligence structures into the decision-making system, the combination of classical methods (HUMINT) with modern digital tools, and a focus on the early detection of threats. It is substantiated that the transformation of Romania's intelligence practices has been driven by the impact of hybrid threats, the digitalisation of the security environment, and the increasing strategic importance of the Black Sea region as a zone of instability. It is demonstrated that the contemporary security provision model is based on an integrated approach that combines national capabilities with mechanisms of allied cooperation. Furthermore, it is determined that the effectiveness of the Romanian security system largely depends on the quality of intelligence analysis, the level of inter-institutional coordination, and the capacity to adapt to the cross-sectoral nature of contemporary threats. The practical significance of the study lies in the potential application of Romania's experience to enhance Ukraine's national security system, particularly in the development of counterintelligence, the integration of analytical capacities, and adaptation to hybrid confrontation.

Key words: National Security, Intelligence, Counter-Intelligence, Romania, HUMINT, Cyber Intelligence, Hybrid Threats, Strategic Assessment, the Black Sea Region, Security Policy.

Introduction

The contemporary security environment in Europe is characterised by a transition from a relatively stable system of international relations to conditions of strategic uncertainty, accompanied by the escalation of interstate confrontation, the expansion of the spectrum of hybrid threats, and the digitalisation of conflict. In such circumstances, the transformation of national security mechanisms assumes particular importance, especially through a reassessment of the role of intelligence activity [1, 2].

This study is based on an institutional and comparative analysis of the Romanian intelligence system, drawing on official strategic documents, legislative frameworks, and secondary analytical sources to identify structural features and functional patterns of intelligence governance.

The Republic of Romania, as a state located on Europe's eastern flank, operates in an environment marked by an elevated level of risk due to its geopolitical position in the Black Sea region, its proximity to an active conflict zone, and the spillover effects of instability in adjacent regions. Empirical analysis indicates that, under these conditions, intelligence activity performs a

system-forming role by обеспечением (providing) continuous threat assessment, early warning, and analytical support for state authorities [1, 3].

The Romanian intelligence community comprises several key institutions, including the Romanian Intelligence Service (SRI), the Foreign Intelligence Service (SIE), the Directorate-General for Defence Intelligence (DGIA), and the General Directorate for Internal Protection (DGPI), each of which performs specialised functions within the national security system.

A distinctive feature of the Romanian model is the institutionalised integration of intelligence structures into strategic decision-making processes. Evidence suggests that this integration is ensured through formal mechanisms such as the Supreme Council of National Defence (CSAT), interagency coordination frameworks, and direct analytical support to executive authorities. These arrangements allow intelligence to function not merely as an instrument of information collection, but as a key component in the formulation and implementation of national security policy.

Theoretical Background

The theoretical foundation of this study is grounded in contemporary approaches to understanding intelligence activity as an integrated component of the national security system, combining the functions of information collection, analysis, and support for strategic decision-making. In the context of the Romanian model, this approach is reflected in the National Defence Strategy of Romania 2020–2024, in which security is defined as the outcome of comprehensive risk management, while intelligence activity is identified as a key instrument for the identification and assessment of such risks (Presidential Administration of Romania, 2020; Sîrbu, M.).

From a methodological perspective, the study is based on the analysis of official documents and reports issued by Romania's intelligence authorities, in particular materials published by the *Serviciul Român de Informații* and the *Serviciul de Informații Externe*, which outline the functional aspects of their activities, the main directions of their work, and the transformation of their approaches to security provision (Serviciul Român de Informații [1] ; Serviciul Român de Informații [2]; Serviciul de Informații Externe).

An important theoretical reference point is the concept of expanded security, according to which threats are considered not solely in military terms, but also within the context of economic, informational, cyber, and social processes. This is evidenced by the inclusion, among recognised threats, of such phenomena as cybercrime, transnational organised crime, information operations, and hybrid influence.

In addition, the study is grounded in the assumption that national security systems are embedded within broader allied structures, as is characteristic of NATO member states. In this context, intelligence activity is regarded as an element of a multi-level system combining national and international security mechanisms (North Atlantic Treaty Organization; President of Ukraine, 2024).

Accordingly, the theoretical foundations of the study reflect a shift from a traditional understanding of intelligence towards its interpretation as a systemic instrument of security governance within a complex and multidimensional threat environment.

Data and Methods

This study is based on a qualitative research design combining institutional analysis, document analysis, and elements of comparative assessment. The methodological approach is aimed at identifying the structural and functional characteristics of the Romanian intelligence system and explaining its role within the broader framework of national security governance.

Data Sources

The empirical basis of the study consists primarily of official and open-source materials. These include strategic documents, legislative frameworks, and institutional reports issued by

Romanian state authorities, as well as analytical publications from international organisations and research centres. In particular, the study relies on:

- the *National Defence Strategy of Romania 2020–2024* as the principal doctrinal document defining the national security framework;
- official publications and reports of the *Serviciul Român de Informații* (SRI) and the *Serviciul de Informații Externe* (SIE);
- publicly available materials concerning cyber intelligence, counterintelligence, counterterrorism, and transnational threats;
- analytical sources related to NATO's eastern flank and Black Sea regional security.

The selection of sources is based on their relevance to the research objectives, their institutional authority, and their capacity to reflect both normative and operational dimensions of intelligence activity.

Methods

The study employs the following methods:

1. **Institutional analysis**, used to examine the structure of the Romanian intelligence community, the distribution of functions among its key actors, and the mechanisms of coordination within the national security system.
2. **Document analysis**, applied to strategic and operational materials in order to identify dominant concepts, threat perceptions, and functional transformations in intelligence practice. This method enables the reconstruction of the logic underlying the Romanian model of security provision.
3. **Comparative approach (limited scope)**, used to contextualise the Romanian model within broader NATO and European security frameworks, particularly with regard to allied integration and multidomain threats.
4. **Analytical generalisation**, employed to synthesise empirical findings and derive conclusions about the systemic features of intelligence governance and security provision.

Analytical Framework

The analysis is guided by the concept of **risk-based and multi-level security governance**, which interprets intelligence as an integrated component of decision-making processes rather than as a purely informational function. Within this framework, particular attention is paid to:

- the role of intelligence in early warning and threat assessment;
- the interaction between intelligence and political decision-making structures;
- the balance between HUMINT and technological intelligence capabilities;
- the integration of national intelligence systems into allied security architectures.

Limitations

The study has several limitations that should be acknowledged. First, it relies predominantly on official and open-source materials, which may reflect institutional perspectives and normative representations rather than fully capture operational realities. Second, the absence of quantitative data limits the possibility of measuring the effectiveness of the intelligence system through formal indicators. Third, the comparative component is limited and does not provide a full cross-national analysis.

Despite these limitations, the selected methodological approach allows for a systematic examination of the Romanian intelligence model and provides a sufficient basis for analytical conclusions regarding its structure, functions, and adaptation to contemporary security challenges.

Results

The contemporary model of security provision in the intelligence practice of the Republic of Romania is shaped by two fundamental factors. The first is the state's geopolitical position as a country on the eastern flank of NATO and the European Union, directly linked to the security of the Black Sea region. The second is the institutional evolution of Romania's security system, within which intelligence has evolved from being merely an instrument of information gathering into a central mechanism for early warning, strategic assessment, and support for state governance. It is for this reason that the National Defence Strategy of Romania 2020–2024 defines security as the outcome of the integrated management of multidimensional risks and threats, while resilience, strategic foresight, and the strengthening of institutional capacities are identified as key state priorities (Presidential Administration of Romania, 2020; Sîrbu, M.).

At the institutional level, the Romanian model is characterised by a relatively clear division of functions among the principal elements of the intelligence community, combined with a strong requirement for coordination. A central role in the domestic sphere is played by the *Serviciul Român de Informații*, which is responsible for safeguarding the constitutional order, conducting counterintelligence activities, countering terrorism, cyber intelligence, the protection of classified information, the prevention of transnational threats, and the identification of risks to national security. In the external domain, the *Serviciul de Informații Externe* operates with core functions that include the collection of intelligence for state decision-making, the provision of early warning on risks and threats in the international environment, and the conduct of operations aimed at protecting and advancing Romania's interests abroad. Both services are coordinated at the strategic level through the *Consiliul Suprem de Apărare a Țării*, which provides a framework for integrated threat assessment and mitigates the risk of fragmentation in information flows (Serviciul Român de Informații [1] ; Serviciul Român de Informații [2]; Serviciul de Informații Externe).

This institutional architecture explains why the contemporary Romanian security model cannot be reduced to the classical division between "internal" and "external" intelligence. In practice, it operates as a system for transforming information into actionable state decisions. Accordingly, the emphasis is placed not only on the collection of information, but also on its processing, analytical interpretation, correlation with multiple sources, and timely dissemination to political and military leadership in a form suitable for decision-making. In this respect, the Romanian model corresponds more closely to contemporary risk-based security governance than to traditional administrative models of intelligence services (Presidential Administration of Romania, 2020; Serviciul Român de Informații [2]).

A characteristic feature of Romanian practice is the predominance of a counterintelligence-oriented approach. This reflects the nature of the threat environment, which extends beyond conventional military risks to include espionage, penetration of strategic sectors, information operations, hybrid sabotage, the exploitation of transnational crime, cyber operations, and the manipulation of public sentiment. Open-source materials from the SRI indicate that particular emphasis is placed on the protection of classified information, industrial security, access vetting, security regime control, and the prevention of information leakage. This suggests that counterintelligence is conceptualised broadly as a multilayered system of state protection rather than merely the detection of hostile agents (Serviciul Român de Informații. *Protecția informațiilor clasificate*).

This conclusion is further supported by the development of the cyber component. Following the adoption of Law No. 58/2023, the SRI has been designated as the nationally competent authority in the field of cyber intelligence, and new categories of threats to national security have been formally recognised. These include cyber-attacks against critical infrastructure, phenomena affecting resilience to hybrid risks, and online propaganda or disinformation campaigns capable of influencing the constitutional order. This development indicates a formal expansion of the intelligence mandate beyond traditional military-political threats, incorporating cyberspace, digital disinformation, and hybrid influence into the core domain of intelligence activity (Serviciul Român de Informații. *Cyberintelligence*.).

At the same time, digitalisation does not eliminate the role of the human factor. Romanian intelligence practice demonstrates the coexistence of technical capabilities with traditional agent-based and counterintelligence methods. This reflects the nature of contemporary threats: while technical tools may detect communications, network intrusions, or anomalies in the information environment, they do not fully explain intent, motivation, recruitment channels, organisational linkages, or the likelihood of escalation from influence to active sabotage. Consequently, HUMINT and counterintelligence penetration remain critically important, particularly in countering foreign influence networks, criminal-intelligence symbioses, and transnational operational schemes (Serviciul Român de Informații. (n.d.). *Amenințări transnaționale*; Serviciul Român de Informații. (n.d.). *SRI foiled a sabotage operation conducted by the Russian Federation*).

A notable example is the information released by the SRI in January 2025 regarding the prevention of a sabotage operation on Romanian territory, which was attributed to the hybrid toolkit of the Russian Federation. According to official statements, the case involved the preparation of sabotage acts by a foreign operative who was identified prior to execution. This case provides empirical evidence that hybrid threats in Romania's security environment are not merely conceptual but manifest in concrete operational activities. Accordingly, security provision increasingly entails not only awareness but also pre-emptive action (Serviciul Român de Informații. (n.d.). *SRI foiled a sabotage operation conducted by the Russian Federation*).

An equally important dimension is counterterrorism. The SRI is designated as the leading national authority for the prevention and counteraction of terrorism, performing functions that include intelligence collection, multi-source analysis, monitoring, interagency coordination, and cooperation with international partners. Methodologically, this indicates that counterterrorism in Romania is structured not as an isolated function of a single agency, but as an integrated intelligence-analytical system aimed at identifying vulnerabilities and risk factors before they materialise into threats (Serviciul Român de Informații. (n.d.). *Preventing and countering terrorism*).

Another significant aspect is the linkage between security and transnational threats. The SRI classifies organised crime, illegal migration, cybercrime, large-scale tax evasion, smuggling, and illicit transfers of military technologies as national security risks. This reflects a key feature of the Romanian approach: intelligence operates at the intersection of internal security, economic stability, and international obligations. As a result, the contemporary model of security provision can be understood as a model of expanded security, encompassing economic, criminal, logistical, and network-related dimensions as potential vectors of destabilisation (Serviciul Român de Informații. (n.d.). *Amenințări transnaționale*).

This expanded security logic is particularly evident in the Black Sea dimension. In recent years, Romania has emerged as a key allied hub of deterrence and security in the region. Analytical assessments indicate that Black Sea security has become central to Romania's strategic outlook. Russia's full-scale war against Ukraine has reinforced this trend, bringing issues such as military mobility, maritime security, protection of transport corridors, allied presence, and regional stability into the core of threat assessment. The bilateral security agreement between Ukraine and Romania

(July 2024), which предусматриє cooperation in intelligence, counterintelligence, cyber security, information security, and Black Sea security, further demonstrates the increasing regionalisation of Romania's security model (North Atlantic Treaty Organization; President of Ukraine, 2024; Reuters).

At the same time, this model should not be idealised. Its strengths — counterintelligence depth, expanded mandate, early warning capabilities, cyber integration, coordination through the CSAT, and strong links with NATO and the EU — are accompanied by structural limitations. These include dependence on allied frameworks in areas where national intelligence capacities are insufficient, the risk of systemic overload due to the expansion of intelligence functions, and challenges related to institutional trust and corruption risks, which may affect public perceptions and the societal legitimacy of the security system (Presidential Administration of Romania, 2020; Sîrbu).

From a scholarly perspective, the Romanian model is best understood not as an ideal type, but as an adaptive security system of a medium-sized state operating under conditions of heightened risk and constrained resources. Its defining feature is the combination of national counterintelligence and analytical capacities with allied integration. In this sense, Romanian intelligence practice reflects a model of "security through integration", where resilience is strengthened both domestically and through participation in broader security frameworks. For Ukraine, this model has practical relevance, demonstrating that effectiveness depends not solely on resource scale, but on coordination quality, the balance between HUMINT and technical capabilities, normative adaptability, and the capacity to integrate intelligence into strategic governance (Presidential Administration of Romania, 2020; Serviciul Român de Informații. (n.d.). Cyberintelligence; North Atlantic Treaty Organization).

Discussion

The results of the study suggest that the Romanian model of intelligence-based security provision reflects a transition from a traditional, functionally segmented system towards an integrated model of security governance. This transformation aligns with broader theoretical perspectives on risk-based and multi-level security systems, in which intelligence is embedded within decision-making structures rather than operating as a separate informational subsystem.

A key implication of the findings is the redefinition of intelligence from a supporting function to a system-forming element of governance. However, this conclusion requires careful qualification. While institutional arrangements such as the CSAT facilitate integration, the degree to which intelligence outputs directly influence political decisions remains dependent on broader governance dynamics, including political priorities and administrative capacity.

The predominance of counterintelligence reflects adaptation to a hybrid threat environment, yet it also raises questions regarding balance. An excessive focus on counterintelligence may potentially limit the development of external intelligence capabilities or strategic forecasting functions. Comparative analysis with other NATO states suggests that successful models tend to maintain a more balanced distribution between counterintelligence, foreign intelligence, and analytical capacities.

The expansion of the intelligence mandate into cyber and informational domains represents a necessary adaptation to contemporary threats. At the same time, this expansion creates risks of functional overload and institutional overstretch. As intelligence agencies assume responsibilities in areas such as cyber resilience, critical infrastructure protection, and disinformation counteraction, the boundaries between intelligence, law enforcement, and regulatory functions become increasingly blurred. This may complicate accountability mechanisms and require further institutional clarification.

The coexistence of HUMINT and technical intelligence confirms the hybrid nature of modern intelligence practice. The findings support the argument that technological capabilities cannot fully

replace human intelligence, particularly in understanding intent and complex organisational behaviour. This has implications for resource allocation, training, and institutional development.

The regional dimension of the Romanian model highlights the growing importance of allied integration. The concept of "security through integration" appears to be a defining feature of medium-sized states operating under conditions of limited resources. However, this also implies a degree of dependency on allied intelligence frameworks, which may constrain national autonomy in certain areas.

An important limitation of the study is its reliance on official and open-source materials, which may reflect institutional narratives rather than fully capture operational realities. Future research should incorporate comparative analysis and independent data sources to provide a more balanced assessment.

In practical terms, the Romanian experience offers relevant insights for Ukraine. The findings indicate that the effectiveness of an intelligence system depends not only on resource capacity, but also on institutional coordination, the integration of analytical functions, and the ability to adapt to hybrid threats. However, the transferability of this model requires careful consideration of contextual differences, including scale, threat intensity, and governance structures.

Conclusions

The contemporary model of security provision in the intelligence practice of the Republic of Romania constitutes an integrated system in which intelligence plays a central role in the formulation and implementation of state security policy. Its principal characteristic lies in the combination of classical intelligence instruments—above all counterintelligence and HUMINT—with modern technological and analytical approaches.

The analysis indicates that the Romanian model is oriented towards the early detection of threats, their systematic interpretation, and their transformation into actionable decisions. At the same time, a counterintelligence-oriented approach remains predominant due to the high level of external influence and hybrid threats. The development of cyber intelligence, integration into allied security structures, and the strengthening of the analytical component further demonstrate the system's adaptation to contemporary challenges.

The practical significance of the Romanian model lies in its demonstration of the effectiveness of an integrated approach to security provision, combining national capabilities with international cooperation. For Ukraine, this experience is particularly relevant in the context of developing intelligence structures, countering hybrid threats, and integrating analytical capabilities into the process of state governance.

Prospects for Further Research

Further research would benefit from a more in-depth analysis of the interaction between intelligence and analytical structures within an integrated security system, particularly with regard to the effectiveness of combining HUMINT and cyber intelligence under conditions of hybrid confrontation. Particular attention should also be given to the mechanisms through which intelligence systems adapt to multidomain threats, as well as to a comparative analysis of the models of Romania, France, and other European Union states, with a view to identifying both universal and nationally specific approaches.

Of practical importance is also the study of the potential for implementing selected elements of the Romanian model within Ukraine's national security system, taking into account wartime conditions and institutional specificities.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

Presidential Administration of Romania. (2020). *National defence strategy of Romania 2020–2024*. https://www.presidency.ro/files/userfiles/National_Defence_Strategy_2020_2024.pdf

Sîrbu, M. (n.d.). *Romania's national defense strategy 2020–2024: A reinforced pillar for NATO*. Center for European Policy Analysis. https://cepa.org/article/romania-national-defense-strategy-2020-2024

Serviciul Român de Informații [1]. (n.d.). *Despre noi*. https://www.sri.ro/despre-noi

Serviciul Român de Informații [2]. (n.d.). *Rapoarte de activitate*. https://www.sri.ro/rapoarte

Serviciul de Informații Externe. (n.d.). *Misiune și atribuții*. https://www.sie.ro/despre.html

Serviciul Român de Informații. (n.d.). *Protecția informațiilor clasificate*. https://www.sri.ro/protectia-informatiilor

Serviciul Român de Informații. (n.d.). *Cyberintelligence*. https://www.sri.ro/cyberintelligence

Serviciul Român de Informații. (n.d.). *Amenințări transnaționale*. https://www.sri.ro/amenintari-transnationale

Serviciul Român de Informații. (n.d.). *SRI foiled a sabotage operation conducted by the Russian Federation*. https://www.sri.ro/en/sabotage-operation

Serviciul Român de Informații. (n.d.). *Preventing and countering terrorism*. https://www.sri.ro/antiterorism

North Atlantic Treaty Organization. (n.d.). *Black Sea security and Eastern flank analysis*. https://www.nato.int/cps/en/natohq/topics_136388.htm

President of Ukraine. (2024). *Security cooperation agreement between Ukraine and Romania*. https://www.president.gov.ua/en/news/security-agreement-ukraine-romania-2024

Reuters. (n.d.). *Black Sea maritime security developments*. https://www.reuters.com/world/europe/black-sea-security