INTELLIGENCE ACTIVITIES IN THE FUNCTION OF NATIONAL SECURITY IN CROATIA

DOI: https://doi.org/10.37458/nstf.26.2.2
Review paper
Received: March 5, 2025
Accepted: June 23, 2025

Sofija Kovač[*], Davor Ćutić[**]

Abstract: This paper examines the role of intelligence operations as one of the pillars of national security in the context of contemporary challenges such as hybrid warfare, cyberattacks, organized crime, and terrorism. Through comparative analysis, case studies, and a descriptive methodological approach, the research analyzes the intelligence system of the Republic of Croatia and compares it to the established models of the United States and the

[*] Sofija Kovač graduated from the Croatian Military Academy as part of the military studies program. She is currently a lieutenant in the Armed Forces of the Republic of Croatia. E-mail: sofija.kova@gmail.com

[**] Assist. Prof. Davor Ćutić, is researcher in the Institute for Security and Defense Studies at the „Dr. Franjo Tudman“. E-email: davor.cutic@sois-ft.hr

Federal Republic of Germany. Special focus is placed on the intelligence cycle and the application of strategic analysis in security-related decision-making. The findings show that Croatia has developed a stable and functional system comprising the Security and Intelligence Agency (SOA), the Military Security and Intelligence Agency (VSOA), and the Office of the National Security Council (UVNS). However, the system faces challenges related to technological modernization, the need for specialized analytical capacities, and stronger parliamentary oversight. The comparison with the U.S. and German systems highlights the importance of enhancing cyber capabilities, increasing transparency, and establishing AI-driven analytical centers capable of processing complex data for early threat detection. The study concludes that further development of intelligence strategies and expansion of international cooperation are essential for effectively responding to new security threats, while maintaining democratic values and institutional accountability.

Keywords: national security, intelligence services, intelligence cycle, strategic analysis, hybrid threats, cybersecurity, international cooperation

Introduction

The global security environment in the 21st century is undergoing significant transformation, driven by rapid technological development, the proliferation of cyber threats, and the evolution of hybrid warfare. In this context, intelligence operations play an indispensable role in protecting national security by enabling the timely detection, analysis, and response to emerging threats (Akrap, 2009). Traditional military capabilities,

while still essential, are no longer sufficient on their own; modern national security increasingly depends on the agility and adaptability of intelligence systems and their ability to cooperate at the international level.

Each country's intelligence apparatus is shaped by its historical experience, security priorities, and political framework. For example, the Croatian intelligence system has developed in the context of post-independence state-building and the legacy of the Homeland War. Tuđman (2001) highlights that the formation of Croatia's intelligence services in the 1990s was crucial for the country's defense and international recognition, emphasizing the formative role intelligence played in safeguarding national sovereignty during its early years.

Today, Croatia's intelligence architecture is based on two principal agencies: the Security and Intelligence Agency (SOA) and the Military Security and Intelligence Agency (VSOA). The SOA primarily handles internal and counterintelligence threats in "civilian" domain, while the VSOA provides military-related intelligence and supports the Ministry of Defense and Armed Forces. Their coordination is ensured through the Office of the National Security Council (UVNS), which aligns intelligence efforts with Croatia's strategic objectives as outlined in its national security framework (Official Gazette, 2017).

In contrast, the United States operates one of the most expansive and technologically advanced intelligence communities in the world, comprising over 17 separate agencies, including the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA). These institutions operate with clearly defined jurisdictions and make extensive use of advanced technologies for data

collection and analysis (Lowenthal, 2017). Germany, on the other hand, has developed an intelligence model characterized by strict legal regulation and parliamentary oversight, with its three main agencies—Bundesnachrichtendienst (BND), Bundesamt für Verfassungsschutz (BfV), and Militärischer Abschirmdienst (MAD)—carefully monitored to prevent abuse of power, a direct consequence of the legacy of the former RSHA (Reichssicherheitshauptamt from the Hitler's Germany) and from the time of GDR and its infamous Stasi apparatus (Akrap, 2011).

Intelligence operations are important part/one of the tools of the intelligence cycle, a structured process that enables the efficient transformation of raw data into actionable intelligence, and strategic analysis, which supports national-level decision-making. These tools are essential for anticipating risks, ensuring timely responses, and enhancing national resilience to both state and non-state threats (Johnson, 2019). Modern intelligence strategies must now confront challenges such as cyber warfare, disinformation campaigns, and transnational organized crime—threats that are increasingly dynamic and asymmetric in nature (ENISA, 2022).

This paper analyzes the role of intelligence operations in the national security system of the Republic of Croatia, situating it in comparison with the more developed and complex systems of the United States and Germany. It further investigates the intelligence cycle, analytical methodologies, and strategic frameworks tailored to contemporary security conditions. By integrating a comparative and evidence-based approach, the objective is to assess the capabilities and limitations of the Croatian intelligence model and to provide opinions for

its modernization and alignment with Euro-Atlantic standards.

Intelligence operations as an element of national security

Intelligence operations represent one of the most critical components of a nation's defense and strategic posture, particularly in the complex security landscape of the 21st century. As modern threats evolve to include cyber warfare, disinformation campaigns, terrorism, and hybrid warfare tactics, traditional defense mechanisms are no longer sufficient. Intelligence services provide the early warning, strategic foresight, and data-driven decision-making support needed to safeguard national interests and maintain public security (Johnson, 2019; Lowenthal, 2017).

The Security and Intelligence System of the Republic of Croatia

The Croatian intelligence and security framework is founded on the Act on the Security and Intelligence System of the Republic of Croatia (Official Gazette,, 2006) which organizes the system around three core institutions: the Security and Intelligence Agency (SOA), the Military Security and Intelligence Agency (VSOA), and the Office of the National Security Council (UVNS).

The SOA is primarily tasked with protecting Croatia's internal security, including counterterrorism, counterintelligence, cybersecurity, and protection of constitutional order (Official Gazette, 79/2006, Article 23). It operates both independently and in cooperation with domestic and international entities to detect and neutralize security threats.

The VSOA, operating under the Ministry of Defence, is responsible for military intelligence. Its functions include collecting, analyzing, and disseminating intelligence relevant to national defense and the operational readiness of the Croatian Armed Forces (Official Gazette, 2006, Article 24).

The UVNS plays a coordinating and oversight role within the intelligence community, ensuring that the operations of SOA and VSOA align with national security policies, strategic interests and Constitution and laws (Official Gazette, 79/2006, Article 6). It also prepares intelligence briefings for the President and Prime Minister and oversees intelligence policy implementation.

The UVNS performs professional and administrative tasks for the National Security Council, the Council for the Coordination of Security-Intelligence Agencies, and administrative tasks for the Coordination for the Homeland Security System, which enable the Council for National Security, the Council for the Coordination of Security-Intelligence Agencies and the Coordination for the Homeland Security System to perform their legally established obligations in the area of national security. (UVNS, 2025)

The scheme 1 illustrates Croatia’s national security structure, highlighting the core institutions (SOA, VSOA, UVNS), functional pillars (intelligence, defense, diplomacy, cybersecurity), strategic oversight bodies, international cooperation mechanisms, and threat categories. Croatia's intelligence architecture is functionally streamlined, which allows for operational efficiency and direct communication between agencies and the executive branch.

The National Development Strategy of the Republic of Croatia until 2030 (Official Gazette, 2021). emphasizes the importance of digital transformation and cybersecurity as integral components of national development. It highlights the need for robust digital infrastructure and the protection of critical information systems, aligning with the paper's discussion on the establishment of a Cyber Command under VSOA and the development of public-private partnerships in cybersecurity (Narodne novine, 2021).

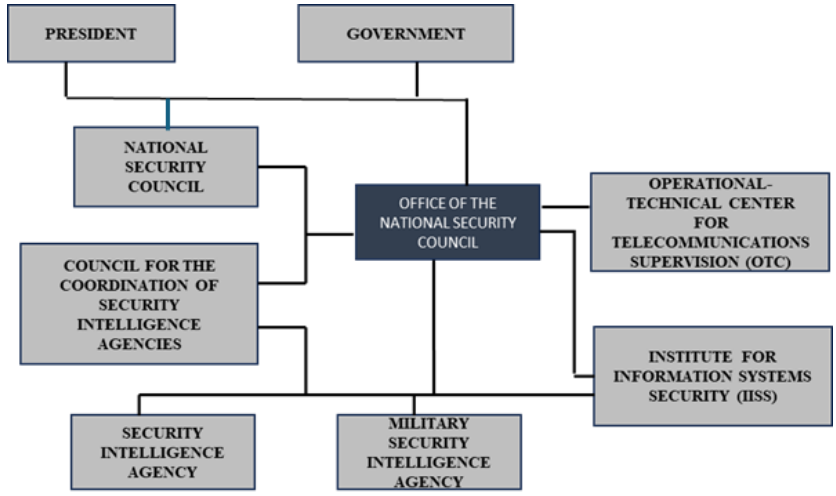

Figure 1: UVNS in the security and intelligence system of the Republic of Croatia, Source: UVNS RH

Intelligence collection includes methods such as human intelligence (HUMINT), signals intelligence (SIGINT), and cyber intelligence, which are then analyzed and converted into strategic insights for decision-makers (Tuđman, 2001). Counterintelligence activities are also vital in defending against foreign espionage and cyber intrusions. Furthermore, Croatia is a committed participant in NATO and EU intelligence-sharing structures, which strengthens its collective defense posture.

Recent developments underscore Croatia's modernization efforts. As of 2023, the government has established a dedicated Cyber Command under the Military Security and Intelligence Agency (VSOA), tasked with cyber defense and critical infrastructure protection (Croatian Government, 2023). The EU Agency for Cybersecurity rates Croatia as 'moderately prepared' while identifying vulnerabilities in its energy infrastructure (ENISA, 2023).

Intelligence Operations in the Context of National Security

In contemporary national security strategy, intelligence is no longer reactive; it is proactive, predictive, and preventative. The National Security Strategy of the Republic of Croatia (Official Gazette, 2017) identifies intelligence capabilities as essential tools for national defense, particularly in the face of non-conventional and asymmetrical threats.

Intelligence operations contribute to national security through several key functions:

- Anticipation of Threats: Early identification of national and international risks, allowing for preventive diplomatic or security action.
- Strategic Planning Support: Supplying political and military leaders with contextual intelligence for policy and operational decision-making.
- Crisis Response: Facilitating rapid assessment and action in times of political, military, or environmental emergencies.
- International Security Engagement: Supporting Croatia’s role in NATO, the EU, and UN peace and security frameworks.

Akrap (2009) emphasizes that modern intelligence operations must also be seen as instruments of

information strategy, aimed at shaping public knowledge and resilience against manipulation and propaganda. In the context of global hybrid threats, intelligence agencies must not only protect against physical harm but also safeguard the information integrity of society.

Emerging Threats and Intelligence Priorities

Modern intelligence operations face a growing array of complex and transnational security challenges:

- Hybrid Threats: These combine military pressure, cyberattacks, economic coercion, and information warfare to destabilize governments and populations. Russia's actions in Ukraine and earlier examples from the Balkans illustrate how hybrid tactics can exploit internal divisions and weak institutions (Akrap, 2011).
- Cybersecurity: Intelligence services are increasingly involved in protecting national infrastructure from cyberattacks, cyber espionage, and data breaches. The European Union Agency for Cybersecurity (ENISA) has consistently warned of the growing risks to state institutions, the energy sector, and financial systems (ENISA, 2022).
- Terrorism and Radicalization: Global terrorist networks continue to use encrypted communications and social media for recruitment and operational planning. Intelligence services must balance surveillance needs with human rights protections while preventing radicalization and monitoring high-risk individuals and groups (Johnson, 2019).

To meet these challenges, modern intelligence operations must adopt innovative collection and analytical tools such as artificial intelligence, big data

analysis, and real-time surveillance systems. Moreover, intelligence cooperation with allies, especially through NATO's Intelligence Fusion Centre, is crucial for maintaining shared situational awareness and coordinated action (NATO, 2023).

As Tuđman (2001) argues, the foundational years of Croatia's intelligence community demonstrated the importance of institutional continuity, public trust, and interagency cooperation—principles that remain just as relevant in the face of today's evolving threats.

Comparison of the Croatian intelligence system with selected countries

National intelligence systems are structured according to each country's geopolitical context, historical legacy, and strategic needs. The Croatian intelligence model, while relatively new, has matured under the influence of Euro-Atlantic integration and is oriented toward democratic accountability, interoperability with NATO and EU partners, and strategic adaptability. To assess its current performance and future prospects, this chapter compares Croatia's intelligence system with the more established systems of the United States and Germany—two countries with differing yet complementary approaches to intelligence, oversight, and global security operations.

Structure of the Intelligence System – Organization and Jurisdiction

The United States operates a highly fragmented but technologically advanced intelligence community, composed of 17 federal agencies, including the Central Intelligence Agency (CIA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Defense Intelligence Agency (DIA). These agencies

operate under the oversight of the Director of National Intelligence (DNI) and are distinguished by specialized mandates and global operational reach (Lowenthal, 2017; Johnson, 2019).

Germany's intelligence structure includes the Bundesnachrichtendienst (BND) for foreign intelligence, the Bundesamt für Verfassungsschutz (BfV) for domestic security and extremism monitoring, and the Militärischer Abschirmdienst (MAD) for military counterintelligence. This tripartite system is governed by strict legal constraints and is deeply influenced by Germany's historical experience with totalitarian intelligence abuse (Riecker, 2020; Akrap, 2011).

Comparative Analysis of Intelligence Systems: Croatia, the USA, and Germany

The intelligence systems of modern states reflect their political culture, constitutional order, and security needs. Although Croatia, the United States of America, and the Federal Republic of Germany share a democratic framework for the functioning of intelligence services, there are significant differences in institutional structure, scope of authority, oversight mechanisms, and international cooperation.

Functional and Institutional Structure

Croatia's intelligence system consists of two main agencies: the Security and Intelligence Agency (SOA), responsible for civilian security, and the Military Security and Intelligence Agency (VSOA), which operates in the defense sector. The system is functionally straightforward, with clearly separated mandates between civilian and military components. It is partially

centralized through the National Security Council and the Office of the National Security Council.

In the United States, the intelligence system is highly complex and includes 18 separate agencies, such as the CIA, FBI, NSA, DIA, and others. A key difference from Croatia and Germany is the existence of the Director of National Intelligence (DNI), who coordinates all agencies. The American system operates within the Intelligence Community, characterized by a high degree of specialization and a division between domestic (e.g., FBI) and foreign intelligence (e.g., CIA).

The German system is decentralized and based on three main services: BND (foreign intelligence), BfV (domestic security), and MAD (military counterintelligence). Unlike the United States, Germany does not have a single overarching authority coordinating all intelligence services. Instead, responsibility is divided between federal and state-level institutions, reflecting its federal political structure.

Parliamentary Oversight and Legal Framework

In Croatia, parliamentary oversight of the intelligence services is conducted by the Parliamentary Committee for Internal Policy and National Security. In theory, there is also a Council for Civilian Oversight of the Intelligence Agencies, but in practice, its influence and institutional strength are underdeveloped.

The U.S. system entails robust parliamentary oversight through the Senate and House Intelligence Committees. In addition, there is judicial oversight via the FISA Court, particularly in surveillance involving U.S. citizens. Nonetheless, due to the broad power and secrecy involved, concerns often arise regarding the

balance between national security and individual privacy.

Germany applies a highly formalized legal approach to intelligence oversight. The Parliamentary Control Panel (PKGr) is authorized to request information and monitor the activities of all services. Furthermore, the Federal Administrative Court may intervene in cases of alleged illegal operations, while the Federal Commissioner for Data Protection and Freedom of Information (BfDI) ensures compliance with fundamental rights. Germany's system strictly limits operational powers, especially regarding surveillance of communications.

International Cooperation and Interoperability

All three countries participate in international security frameworks such as NATO, but their approaches to cooperation differ. Croatia relies on data sharing with EU and NATO members and participates in regional initiatives such as SELEC. In terms of technical interoperability, Croatia depends largely on the support of allied countries.

The United States maintains the most extensive network of international intelligence cooperation in the world, including the Five Eyes alliance and global capabilities in electronic surveillance, cryptography, and cyber defense. U.S. agencies frequently play a leading role in coordinating with partner nations.

Germany cooperates primarily within EU and NATO frameworks, with strong emphasis on constitutional constraints and personal data protection. Although it utilizes U.S. resources (e.g., for SIGINT), Germany prefers a legally formalized and bilateral approach to information exchange.

Croatia possesses a compact intelligence system with core functions but lacks sufficiently developed models of oversight and international reach. The United States operates a comprehensive, technologically dominant, and politically influential system, yet it faces challenges related to transparency and control. Germany is developing the most legally restrictive system, where the protection of rights and institutional oversight are fundamental values, though this comes at the cost of some operational flexibility.

To highlight institutional distinctions, the next table compares the intelligence systems of Croatia, the United States, and Germany in terms of structure, function, and oversight.

Table 1. Structure of Intelligence Systems in Croatia, the United States, and Germany

Country	**Key Intelligence Agencies**	**Primary Responsibilities**	**Parliamentary Oversight**
Croatia	SOA, VSOA, UVNS	Internal/external security, military intelligence, coordination	Parliamentary Committee for Internal Policy and National Security, Council for Civilian Oversight of Security and Intelligence Agencies Croatian Parliament, (2024.)
U.S.	CIA, NSA, FBI, DIA	Foreign intelligence, cybersecurity, counterintelligence, defense analysis	House and Senate Intelligence Committees

Country	Key Intelligence Agencies	Primary Responsibilities	Parliamentary Oversight
Germany	BND, BfV, MAD	Foreign threats, domestic extremism, military security	Bundestag Parliamentary Control Committee

Source: Adapted from Lowenthal (2017); Johnson (2019); Riecker (2020); Official Gazette (2006)

Croatia's system, while modest in size, benefits from clarity in agency responsibilities and centralized oversight. However, it lacks the specialized substructures present in larger intelligence systems, such as the NSA in the U.S. or Germany's Federal Office for Information Security (BSI).

Oversight Models and Intelligence Accountability

Effective democratic oversight is a cornerstone of legitimate intelligence operations and essential for the prevention of abuse of power. Croatia's intelligence system is overseen by the Parliamentary Committee for Internal Policy and National Security, which monitors the activities of the SOA and VSOA. Parliamentary oversight has the right to full insight into all documents and activities of all intelligence services. However, limitations remain in terms of operational transparency and the depth of parliamentary review processes, which can hinder the full realization of democratic control.

In addition to parliamentary mechanisms, the system includes the Council for Civil Oversight, the oversight of the Office of the National Security Council (UVNS), and judicial oversight by Supreme Court judges who authorize intrusive measures. The role of the media in monitoring and reporting on broader accountability must

also be acknowledged. All these layers of oversight need to be emphasized as part of a robust democratic framework.

Nonetheless, it is important to underline that transparency regarding operational activities—such as methods, goals, techniques, and technology—toward the public and the media must not exist, as it would undermine the very purpose and effectiveness of intelligence services.

In the United States, congressional oversight is robust, conducted through the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. These bodies hold public hearings, authorize budgets, and scrutinize executive actions, particularly post-9/11 reforms that strengthened accountability mechanisms (Johnson, 2019).

Germany stands out for its rigorous parliamentary oversight. Its intelligence services are subject to the Parliamentary Control Panel (PKGr), which has broad authority to review classified operations, a framework developed in response to past abuses by the RSHA and Stasi (Akrap, 2011; Riecker, 2020).

While the U.S. model emphasizes efficiency and technical superiority, and Germany stresses legal control and transparency, Croatia can benefit from incorporating best practices from both systems to enhance democratic governance of intelligence.

Operational Capabilities and International Cooperation

Croatia participates actively in NATO, the EU Intelligence and Situation Centre (EU INTCEN), and various bilateral and multilateral agreements and clubs (Hänni, 2018). Its capabilities are largely focused on

regional threats and defense cooperation within the Euro-Atlantic sphere (Official Gazette, 2017). However, it lacks the global surveillance infrastructure or cyber-specific institutions like the NSA (U.S.) or Germany's BSI, which limits autonomous response to global cyber threats (ENISA, 2022).

The United States maintains unparalleled intelligence reach, with satellite surveillance, cyber command capabilities, and human intelligence networks that span the globe. Its technological superiority is reinforced by the integration of artificial intelligence, big data analytics, and cyber operations across military and civilian intelligence sectors (Lowenthal, 2017).

Germany, while more Europe-focused, is a critical player in counterterrorism and cyber defense. Its agencies collaborate with both EU and NATO partners and prioritize data protection and operational legality, maintaining a balance between capability and civil rights (Riecker, 2020).

Croatia's strengths lie in its interoperability with allies and a clear legal framework. However, it must continue building capacity in strategic analysis, cyber defense, and advanced signal intelligence to meet evolving threats effectively (Akrap, 2009).

Challenges and Recommendations for the Croatian Intelligence System

While Croatia's intelligence system performs well within its regional scope, a comparative analysis reveals several areas for improvement:

"Cybersecurity Specialization: Establish a dedicated national cybersecurity body, similar to the NSA or Germany's BSI, to address sophisticated cyber threats and infrastructure vulnerabilities. A cyber center has

already been established within the SOA which, when fully developed, is intended to become an independent government body." (ENISA, 2022; SOA, 2025).

Enhanced Parliamentary Oversight: Introduced structured review mechanisms and regular performance audits of SOA and VSOA, modeled after Germany's Bundestag system (Akrap, 2011; Riecker, 2020).

Strategic International Engagement: Expand cooperation beyond NATO/EU by building intelligence-sharing frameworks with like-minded states and global cybersecurity networks.

Capacity Building and Technological Modernization: Invest in AI-based data analytics, satellite imagery processing, and open-source intelligence (OSINT) capabilities to strengthen situational awareness and early warning systems (Tuđman, 2001).

Public Trust and Transparency: As Akrap (2009) notes, shaping public knowledge through information strategy enhances democratic legitimacy and resilience. Croatia should promote responsible communication and civic education on intelligence and security matters to reinforce trust in its intelligence and security institutions.

Intelligence cycle and strategic analysis

Intelligence operations are structured around the systematic processing of information to identify, assess, and respond to risks and threats. The intelligence cycle is the central framework guiding these processes. It consists of a sequence of interrelated phases—from planning to dissemination—that ensure the timely flow of relevant intelligence to decision-makers. This cycle in Figure 2 is crucial for achieving strategic foresight and enabling evidence-based decision-making in the field of national and international security (Lowenthal, 2017).

Strategic analysis within intelligence systems relies on advanced methods of interpretation, modeling, and risk assessment. It transforms raw data into actionable knowledge, enabling states to anticipate crises, prevent escalation, and design long-term security strategies (Johnson, 2019; Akrap, 2009).

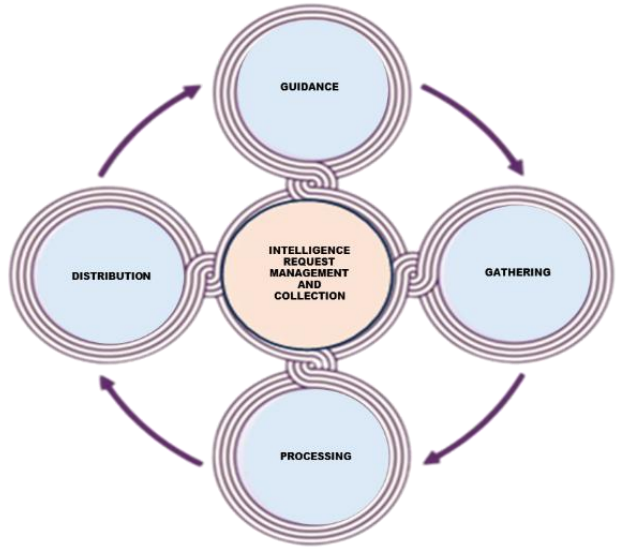

Figure 2: The Intelligence Cycle, Source: (ZDP-20, 2014; Kovač, 2021.)

The Intelligence Cycle – Definition and Phases

The intelligence cycle comprises five core stages, forming a continuous and adaptable model of data processing:

- planning and direction: Defining intelligence priorities and operational goals in alignment with national security strategies.
- data collection: Acquiring information from diverse sources.

- processing and analysis: Filtering, organizing, and evaluating raw data to derive patterns and assess credibility (Riecker, 2020).
- production of intelligence assessments: Generating threat assessments and policy briefings tailored to decision-makers' needs (Johnson, 2019).
- dissemination and Application: Delivering intelligence outputs to political and military leadership through secure channels and in a timely manner (Official Gazette, 2017).
- evaluation (of tasks received, achieved, quality, legality, efficiency)

This cyclical approach ensures continuity in information flow and responsiveness to evolving security demands. It also allows for iterative adjustments based on feedback and newly emerging intelligence.

Methods and Sources of Intelligence Data Collection

Effective intelligence work depends on the appropriate integration of multiple data collection disciplines. Each method offers distinct advantages and limitations in operational scope and reliability:

- HUMINT: Provides nuanced, contextual information through human sources (Lowenthal, 2017). It is indispensable for understanding adversarial intent but carries risks of misinformation and operational compromise.
- SIGINT: Enables rapid monitoring of electronic communications and data flows, but may face encryption or legal barriers (Johnson, 2019).
- OSINT: Leverages publicly available data, including media reports, social media activity, and academic publications (ENISA, 2022). It is

cost-effective and broad in scope but susceptible to manipulation and disinformation.

- IMINT: Offers visual reconnaissance via satellite and aerial imaging, useful in monitoring military infrastructure or natural disaster impact (Riecker, 2020).
- MASINT: Delivers highly technical data, often from sensors detecting radiation, acoustics, or chemical signatures. It provides unique insights but requires specialized infrastructure (Aid, 2012).

Table 2: Advantages and Limitations of Different Intelligence Methods

Method	**Advantages**	**Limitations**
HUMINT	Deep understanding of intentions	Risk of disinformation, recruitment difficulty
SIGINT	Real-time and voluminous data	Legal issues, encryption complexity, Risk of disinformation
OSINT	Open access, scalable	False data risk, noise filtering
IMINT	Strategic and visual insight	Weather-dependent, image quality limits
MASINT	Scientific precision	Technically complex, resource-intensive

Source: Authors, based on verified literature

The combination of these methods enables multidimensional threat assessments. Their cross-validation strengthens the reliability of intelligence products and supports integrated situational awareness.

Intelligence Data Analysis

Strategic analysis is the linchpin of intelligence processing. It ensures that collected data are transformed into valuable insights that inform decision makers. This process goes beyond raw fact-gathering by identifying patterns, assessing risk, modeling outcomes, and forecasting threats.

Methods of Intelligence Analysis

The analysis of intelligence data consists of a five-step methodological process:

Collection of Raw Data: Involves integrating multiple source types (HUMINT, SIGINT, OSINT, etc.) for a comprehensive intelligence picture (Lowenthal, 2017).

Organization and Filtering: Includes classifying, sorting, and verifying data to minimize redundancy and noise using digital tools and expert review (Tuđman, 2001).

Application of Analytical Techniques Encompasses:

- Scenario analysis,
- SWOT analysis,
- Predictive analytics, and
- Inductive/deductive reasoning (Johnson, 2019; Akrap, 2009).

Production of Assessments: Structured intelligence reports are produced with clear recommendations for tactical or strategic decisions (Riecker, 2020).

Dissemination: Reports are distributed through secure networks to policymakers, the armed forces, or international partners (Official Gazette, 2017).

In table 3 authors compare methods and intelligence analysis. This framework fosters intelligence clarity, reduces uncertainty, and enhances decision advantage.

Table 3: Methods of Intelligence Analysis

Phase	**Description**	**Key Tools and Methods**
1. Raw Data Collection	Integrating source data	HUMINT, SIGINT, OSINT
2. Filtering & Organization	Verifying and prioritizing	Data software, analytic vetting
3. Analytical Methods	Modeling and pattern detection	Scenario analysis, AI tools
4. Intelligence Assessments	Drawing conclusions	Strategic and predictive modeling
5. Dissemination	Reporting findings	Secure briefings, distribution of Intelligence, visualizations

Source: Authors

The Role of Strategic Analysis in Decision-Making

Strategic intelligence is used across various sectors, reflecting its interdisciplinary importance:

Table 4 compares highlight the role of strategic analysis in decision making in sectors of national security, defense, diplomacy and cybersecurity. For example, diplomatic intelligence is often used to assess global trends in alliance behavior or instability (Akrap, 2011). In cybersecurity, intelligence aids in understanding attack vectors and protecting digital sovereignty (ENISA, 2022).

Moreover, intelligence plays an increasingly important role in the economic and financial sectors, where it supports the detection of illicit financial flows and anticipates economic shocks that may affect national security (Tuđman, 2001).

Table 4: The Role of Strategic Analysis in Decision-Making

Sector	Application of Strategic Analysis
National Security	Preventing terrorism, securing critical infrastructure
Defense	Military planning, battlefield awareness
Diplomacy	Forecasting geopolitical changes
Cybersecurity	Detecting cyber threats, protecting networks

Source: Authors

Finally, the intelligence cycle and strategic analysis represent foundational pillars of national security architecture. Through structured data collection, advanced analytical methodologies, and tailored dissemination, intelligence supports a broad range of governmental and defense operations. For Croatia, continued investment in analytical capabilities, interagency coordination, and technological modernization remains vital for maintaining situational awareness and responding to emerging threats in an increasingly complex global security environment.

Intelligence strategies and contemporary challenges

In the contemporary security landscape, intelligence strategies are essential for anticipating, preventing, and neutralizing threats to national security. These strategies

provide a framework through which intelligence services align operational priorities, apply modern analytical tools, and adapt to evolving challenges. Their formulation is based on continuous assessment of the strategic environment, the identification of emerging risks, and the integration of technological advances into national security policy (Lowenthal, 2017; Johnson, 2019).

In recent years, intelligence agencies worldwide have had to confront increasingly sophisticated threats—from cyberattacks and disinformation campaigns to organized crime and transnational terrorism. These challenges demand both long-term planning and the agility to respond to dynamic situations in real time. Effective intelligence strategies thus combine foresight, adaptability, and cooperation at the national and international levels (Akrap, 2009; ENISA, 2022).

Intelligence Strategies – Definition and Importance

An intelligence strategy refers to the structured and purposeful use of intelligence resources to defend national interests and guide the operations of intelligence services. Core elements include risk identification, strategic foresight, innovation in intelligence methods, and multilateral cooperation. The integration of artificial intelligence, big data analytics, and cybersecurity protocols has become a critical component of modern strategy (ENISA, 2022).

In the Croatian context, Tuđman (2001) emphasized that intelligence strategies must build institutional resilience and foster interagency coordination to address security threats effectively. Croatia's early intelligence development stressed strategic planning as a key element of sovereignty, a principle that remains relevant in the face of contemporary asymmetric threats.

Key functions of intelligence strategies are presented in table 5 comparing roles of each function in intelligence processing. To remain effective, strategies must be flexible and forward-looking, ensuring the intelligence system remains both robust and adaptable to unforeseen developments.

Table 5: Key Functions of Intelligence Strategies

Function	Description
Prevention	Anticipating and detecting potential threats in a timely manner
Data Collection	Using diverse intelligence sources (HUMINT, SIGINT, OSINT, etc.)
Analysis & Evaluation	Converting data into actionable intelligence
Response to Threats	Implementing countermeasures, interventions, or preemptive actions
International Cooperation	Exchanging intelligence with partners and allied organizations

Source: Authors, based on verified sources

Key Intelligence Strategies

Countries typically adopt several overarching intelligence strategies:

- **Denial Strategy**: Focuses on protecting sensitive information, infrastructure, and technologies from adversaries. This strategy emphasizes counterintelligence, encryption, and security policy to mitigate espionage and cyber intrusions.

- **Engagement Strategy**: Centers on building alliances and multilateral intelligence-sharing networks, particularly in the context of NATO, EU, and UN cooperation. Croatia has increasingly emphasized engagement through its NATO and EU membership, participating in joint operations and analytical platforms (Official Gazette, 2017).
- **Reform Strategy**: Involves the continuous modernization of intelligence capabilities to respond to emerging risks. This includes organizational restructuring, investment in AI and cyber units, and legal reforms to ensure transparency and democratic control (Akrap, 2009).

These strategic pillars allow intelligence systems to adapt to changing threat environments, strengthen international partnerships, and ensure operational resilience.

Contemporary Security Challenges

Hybrid Threats

Hybrid threats are characterized by a mix of conventional and non-conventional tactics—including cyber operations, disinformation, economic pressure, and covert actions—used to destabilize societies. As Akrap (2011) has noted, these threats are particularly dangerous in transitional democracies, where societal trust and institutional stability may be vulnerable.

Examples of hybrid strategies include:

- Russia's involvement in Ukraine, where cyberattacks and media disinformation were combined with conventional military aggression

to undermine sovereignty and public trust (Riecker, 2020).
- Chinese cyber operations have been linked to long-term industrial and political espionage targeting strategic technologies in Western institutions (ENISA, 2022).

To counter hybrid threats, intelligence systems must combine traditional intelligence and counterintelligence methods with digital forensics, AI-supported disinformation tracking, and public resilience initiatives.

Cybersecurity

Cybersecurity has emerged as one of the most critical dimensions of national intelligence. State and non-state actors have developed highly sophisticated cyber tools that can disrupt public services, compromise national infrastructure, and erode public trust.

Key cybersecurity intelligence strategies include:

- Establishing national cybersecurity centers with real-time monitoring capabilities.
- Public-private partnerships for data protection and infrastructure defense.
- Implementing advanced encryption standards and information-sharing platforms across sectors (ENISA, 2022; Lowenthal, 2017).

Croatia's participation in EU cybersecurity mechanisms and the work of the SOA in coordinating cyber defence and policy are vital for mitigating these risks (Official Gazette, 2017).

Terrorism and Organized Crime

Terrorist organizations and transnational criminal groups continue to pose significant threats, particularly as they increasingly exploit digital tools for recruitment, financing, and operational planning:

- Groups such as ISIS and Al-Qaeda have used encrypted platforms and social media to disseminate propaganda and radicalize followers (Johnson, 2019).
- Organized crime networks, including cartels in Latin America, are increasingly turning to cryptocurrencies and encrypted communication platforms to evade detection and finance illicit activities (Riecker, 2020).

To combat these threats, intelligence agencies must strengthen their financial intelligence units, develop digital surveillance techniques within legal frameworks, and deepen international judicial and intelligence cooperation.

In 2023, Croatia's energy grid was targeted by advanced persistent threat groups associated with Russian-aligned cyber actors, emphasizing the need for improved cyber defense coordination (Microsoft, 2023).

The strategy also underscores the importance of international cooperation, particularly within the EU and NATO frameworks. This aligns with the paper's references to Croatia's participation in NATO's Cyber Rapid Reaction Teams and collaboration with the EU Hybrid Fusion Cell (Narodne novine, 2021). Croatia's participation in NATO's Cyber Rapid Reaction Teams and collaboration with the EU Hybrid Fusion Cell demonstrates active involvement in multilateral threat mitigation (NATO, 2023; EEAS, 2023).

As Tuđman (2001) emphasized, intelligence in a democratic state must also uphold constitutional principles and human rights while remaining proactive and preemptive in nature.

Modern intelligence strategies are the cornerstone of effective national security in an era defined by hybrid conflict, digital vulnerability, and asymmetric threats. Croatia, while a relatively small country, has a robust and evolving intelligence framework shaped by its post-independence experiences and Euro-Atlantic integration. Going forward, it must continue to strengthen its analytical capacity, expand international cooperation, and embed technological innovation into its strategic doctrine. Intelligence strategies must remain agile and ethical, ensuring both the safety of the state and the preservation of democratic values.

Conclusions

This paper has explored the role of intelligence operations as one of the foundational pillars of national security, with a particular focus on the intelligence system of the Republic of Croatia. Intelligence services plays a critical role in identifying threats, helping strategic decisions, and preserving democratic stability in the face of contemporary challenges.

Croatia has developed an operationally functional intelligence system composed of the Security and Intelligence Agency (SOA), the Military Security and Intelligence Agency (VSOA), and the Office of the National Security Council (UVNS). These institutions work in concert to coordinate national intelligence efforts, guided by the legal framework established in the Law on the Security and Intelligence System and the National Security Strategy of the Republic of Croatia. While structurally coherent, this system still faces

challenges including limitations in technological capability, and insufficient specialization in cybersecurity.

The National Development Strategy of the Republic of Croatia until 2030 (NN 13/2021, 2021) complements and reinforces the assertions made in the paper regarding the evolution and strengthening of Croatia's intelligence and cybersecurity sectors. It provides a strategic framework that supports the initiatives and developments discussed in the paper, without necessitating any revisions to its content. (Official Gazette, 2021)

One of the strategic objectives of the National Development Strategy is to enhance national security and resilience to crises. This includes strengthening the capabilities of security and intelligence services, which supports this paper's emphasis on the modernization and increased accountability of Croatia's intelligence apparatus (Official Gazette, 2021).

In response, Croatia has initiated reforms aimed at increasing accountability of intelligence services. Transparency International (2024) highlights ongoing legislative proposals to strengthen parliamentary scrutiny, addressing longstanding oversight weaknesses.

The comparison with the intelligence models of the United States and Germany revealed important lessons. The United States' intelligence community, comprising 17 agencies, demonstrates the advantages of technological integration, global reach, and specialization. Germany’s model emphasizes the importance of transparency, rule of law, and strong parliamentary oversight—developed as a response to historical misuse of intelligence structures. These

models offer insights that can support the continued development of Croatia's own system.

A forward-looking analysis of intelligence strategies highlighted the need for adaptability in the face of complex security threats—such as hybrid warfare, disinformation campaigns, cyberattacks, and transnational (organized) crime. Contemporary challenges require innovation, resilience, and broader international coordination. Intelligence services must be capable not only of gathering and analyzing information but also of preventing strategic surprises through anticipatory governance and interagency cooperation.

In this context, Croatia's intelligence system must advance in several key areas. Expanding cooperation with NATO, the EU, and trusted bilateral partners will strengthen Croatia's real-time threat awareness and intelligence exchange. At the same time, transparency and public trust in intelligence institutions must be cultivated through secure information sharing in order to protect critical infrastructures, and responsible communication with publicity. Cooperation with the private sector and academic institutions should also be institutionalized to expand analytical expertise and innovation in intelligence-led security.

Ultimately, the success of national intelligence operations depends on the ability to anticipate evolving security threats, apply strategic and analytical depth, and engage internationally without compromising the values of democracy, legality, and institutional accountability. Croatia has laid a solid foundation for its intelligence architecture, but the coming decade will require continued modernization, integration of new technologies, and unwavering commitment to upholding democratic norms within the security domain.

Literature:

1. Aid, M. (2012). The secret sentry: The untold history of the National Security Agency. Bloomsbury Press.
2. Akrap, G. (2009). Informacijske strategije i oblikovanje javnoga znanja [Information strategies and shaping public knowledge]. National Security and the Future, 10 (2), 77-151. Retrieved July 27, 2025, from https://hrcak.srce.hr/80639
3. Akrap, G. (2011). Cooperation between intelligence and security systems of German Democratic Republic and Yugoslavia. National Security and the Future, 12 (1-2), 35-57. Retrieved July 27, 2025, from https://hrcak.srce.hr/89521
4. Croatian Parliament, (2024.) 11th term of the Croatian Parliament (16 May 2024). Council for Civilian Oversight of Security and Intelligence Agencies. Croatian Parliament. Retrieved July 27, 2025, from https://www.sabor.hr/en/committees/council-civilian-oversight-security-and-intelligence-agencies-11-term
5. ENISA – European Union Agency for Cybersecurity. (2022). Threat landscape report. Retrieved July 27, 2025, from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
6. Hänni, A. (2018). Prequel to the present - multilateral clubs and the secret history of international counterterrorism cooperation in Western Europe, 1969-1989. National Security

and the Future, 19 (1-2), 65-109. Retrieved July 27, 2025, from https://hrcak.srce.hr/clanak/303485

7. Johnson, L. K. (2019). Spy watching: Intelligence accountability in the United States. Oxford University Press.
8. Lowenthal, M. M. (2017). Intelligence: From secrets to policy (7th ed.). CQ Press.
9. NATO. (2023). Intelligence and security policies in NATO framework. NATO Allied Command Transformation. Retrieved July 27, 2025, from https://www.nato.int/cps/en/natohq/
10. Official Gazette, (2021) Nacionalna razvojna strategija Republike Hrvatske do 2030. godine. [National Development Strategy of the Republic of Croatia until 2030] NN 13/2021 (11.2.2021.).
11. Official Gazette. (2006). Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske, Zakon br. 79/2006. [Law on the Security and Intelligence System of the Republic of Croatia]. Retrieved July 27, 2025, from https://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html
12. Official Gazette. (2017). Strategija nacionalne sigurnosti Republike Hrvatske [National Security Strategy of the Republic of Croatia]. Narodne novine, br. 73/2017. Retrieved July 27, 2025, from https://narodne-novine.nn.hr/clanci/sluzbeni/2017_07_73_1772.html
13. Riecker, A. (2020). German intelligence agencies and counterterrorism efforts. Springer.

14. SOA (2025). Kibernetička sigurnost. Sigurnosno–obavještajna agencija Republike Hrvatske. [Security and Intelligence Agency of the Republic of Croatia] Retrieved July 27, 2025, https://www.soa.hr/hr/podrucja-rada/kiberneticka-sigurnost/

15. Tuđman, M. (2001). HIS: 1993–1998 – Prvih pet godina Hrvatske izvještajne službe. National Security and Future, 1. Retrieved July 27, 2025, from https://hrcak.srce.hr/file/343046

16. UVNS – Ured Vijeća za nacionalnu sigurnost. (2025). Podrška Vijeću, Savjetu i Koordinaciji. Retrieved July 27, 2025, from https://www.uvns.hr/hr/o-nama/shema-uvns-u-sigurnosno-obavjestajnom-sustavu-rh

Additional References (2023–2024)

17. Hrvatska vlada. (2023.). Izvješće o provedbi Nacionalne strategije kibernetičke sigurnosti. Croatian Government. (2023). National Cybersecurity Strategy Implementation Report. Retrieved from https://vlada.gov.hr/sjednice/234-sjednica-vlade-republike-hrvatske-38689/38689

18. ENISA – European Union Agency for Cybersecurity. (2023). National Cybersecurity Landscape: Croatia. Retrieved July 27, 2025, from https://www.enisa.europa.eu/topics/national-cyber-security-strategies

19. Transparency International Croatia. (2024). Accountability of Security Services in the

Western Balkans. Retrieved July 27, 2025, from https://www.transparency.org

20. NATO. (2023). Balkan Intelligence Sharing Initiative. Retrieved July 27, 2025, from https://www.nato.int/cps/en/natohq/topics_49188.htm
21. EEAS. (2023). EU Hybrid Threat Report: Eastern Flank Vulnerabilities. Retrieved July 27, 2025, from https://www.eeas.europa.eu/eeas/hybrid-threats_en
22. ODNI. (2023). Annual Threat Assessment of the U.S. Intelligence Community. Retrieved July 27, 2025, from https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf
23. Deutscher Bundestag. (2024). Neue Aufsichtsgesetze für den BND (Drucksache 20/8627). Deutscher Bundestag. Retrieved July 27, 2025, from https://dserver.bundestag.de/btd/20/086/2008627.pdf
24. RAND Corporation. (2024). AI in intelligence: Global trends. RAND Corporation. Retrieved July 27, 2025, from https://www.rand.org/publications Retrieved from
25. Microsoft. (2023). Cyber threats to Eastern European energy grids. Microsoft. Retrieved July 27, 2025, from https://www.microsoft.com/security/blog