Counterintelligence Reform in Southeastern Europe: A Strategic Imperative for Democratic Resilience and National Sovereignty

Abstract

Southeastern Europe occupies a strategically exposed position between Euro-Atlantic institutions, the Western Balkans, the Black Sea and the Eastern Mediterranean. Foreign intelligence activity in this environment may involve traditional espionage, cyber-enabled collection, covert influence, strategic corruption, insider threats and the exploitation of institutional vulnerabilities. This article examines the counterintelligence arrangements of Greece, Albania, North Macedonia, Montenegro, Kosovo, Serbia, Bosnia and Herzegovina, and Bulgaria.

Using a qualitative comparative policy-analysis approach, the article draws on academic literature, publicly available legislation, institutional material and selected documented cases. It finds that counterintelligence functions and legal mandates exist in all eight states, but that they are organised through different combinations of civilian intelligence services, military bodies, police institutions, cybersecurity authorities and coordinating mechanisms. The principal regional issue is therefore not the universal absence of counterintelligence capacity. It is the varying ability of national systems to integrate information, clarify responsibilities, provide strategic warning and maintain effective democratic oversight.

The central argument is that counterintelligence should be treated as a coherent strategic capability rather than merely as one operational function among many, but that the institutional means of achieving that capability should be country-specific rather than uniform across the region.. Depending on existing institutions and available capacity, appropriate measures may include strengthening a current service, clarifying statutory mandates, improving inter-agency coordination, developing specialist analytical capacity or, in limited circumstances, creating a dedicated coordinating body or agency. Any expansion of operational capability should be accompanied by proportional improvements in parliamentary, judicial and independent oversight. Counterintelligence reform is therefore best understood as a differentiated process of institutional development intended to strengthen both national resilience and democratic accountability.

Keywords: Counterintelligence; Southeastern Europe; Intelligence Reform; Democratic Oversight; Hybrid Threats; Foreign Interference; Strategic Warning.

Introduction

Southeastern Europe has entered a security environment in which counterintelligence can no longer be treated as a narrow, technical, or secondary function of the state. The region's geopolitical position, inability to resolve political disputes, uneven institutional resilience, exposure to external influence, and increasing dependence on digital infrastructure have all widened the space of operation for hostile intelligence activity. Espionage, cyber-enabled intrusions, covert political influence, strategic corruption, disinformation, facilitation of organised crime, and the targeting of critical infrastructure increasingly form part of a single threat continuum (Putter and Bachmann, 2022).

The present article addresses the following research question: how can the eight states examined develop more coherent counterintelligence capacity while accounting for differences in institutional design, resources, threat exposure and democratic governance? The central argument is that counterintelligence should be treated as a coherent strategic capability rather than merely as one operational function among many. The institutional means of achieving that capability, however, should differ according to national threat exposure, existing intelligence architecture, available resources and democratic-governance capacity. The eight-country comparison is therefore intended to capture variation in institutional configuration rather than to establish regional institutional uniformity. To answer the research question, the analysis first distinguishes counterintelligence from the broader concepts of intelligence and hybrid-threat response. It then compares existing national arrangements and selected cases before evaluating the risks of fragmentation, institutional concentration and political misuse. For the purposes of this article, Southeastern Europe refers specifically to Greece, Albania, North Macedonia, Montenegro, Kosovo, Serbia, Bosnia and Herzegovina, and Bulgaria. This definition is analytical rather than an assertion that these states constitute a homogeneous political or security bloc. The eight cases are considered together because they occupy an interconnected strategic space in which cross-border infrastructure, economic relationships, organised-crime networks, political disputes, information environments and competing external influences interact, while their national institutional arrangements remain markedly different. They are not treated as being at a common stage of political or institutional development, nor as facing equivalent configurations of threat. On the contrary, variation in constitutional structure, intelligence architecture, international alignment, administrative capacity and democratic oversight forms part of the comparative design. The analytical purpose of examining the eight states together is therefore to assess how different national institutional configurations address the higher-order problem of converting counterintelligence responsibilities into strategic assessment, warning, coordination and accountable action, rather than to derive a single regional institutional prescription. This article adopts a qualitative, comparative policy-analysis approach. It draws on peer-reviewed scholarship in intelligence studies, counterintelligence, democratic security-sector governance, hybrid threats and cybersecurity, together with publicly available reports issued by European and Euro-Atlantic institutions. The analysis also uses selected national examples to illustrate differences in institutional design, threat exposure and democratic safeguards across the eight states under examination. The article does not draw on classified material, operational reporting, interviews or original fieldwork. Its purpose is therefore not to assess the effectiveness of undisclosed counterintelligence operations or to rank national services. Instead, it evaluates publicly observable institutional arrangements, legal and oversight principles, documented vulnerabilities and policy responses. Official institutional reports are treated as evidence of the assessments and priorities of the organisations that produced them, rather than as automatically neutral or exhaustive accounts.

Where possible, their claims are considered alongside academic analysis and evidence from more than one source. The cases discussed in the article are illustrative rather than statistically representative. They are used to identify recurring institutional problems and differences among national contexts, not to imply that all eight states experience identical threats or possess equivalent capacities. The resulting recommendations should consequently be understood as conditional policy pathways whose suitability depends on each state's legal framework, institutional structure, resources and democratic safeguards. The intended policy community for this analysis comprises national-security policymakers, intelligence and security-sector leadership, officials responsible for inter-agency coordination, parliamentary and independent oversight bodies, and international partners involved in security-sector capacity-building. Its practical contribution is not to prescribe a common organisational model, but to provide criteria for identifying whether a national reform problem lies primarily in mandate, coordination, analytical capacity, resources or oversight, and for linking that diagnosis to an appropriate institutional pathway.

This article also examines whether the changing threat environment affecting the eight states defined above requires counterintelligence to be developed as a more coherent strategic capability. It does not propose a uniform institutional solution. Depending on each state's legal framework, existing intelligence architecture, threat profile, administrative capacity, and oversight arrangements, reform may involve strengthening an existing service, establishing a national coordinating centre, clarifying statutory responsibilities, or improving formal mechanisms for inter-agency The functions of counterintelligence do exist in regional intelligence and security systems but they are often fragmented, embedded within wider services or subordinated to police, military or general intelligence priorities. This institutional dispersion may reduce strategic coherence, when hostile intelligence activity is becoming more complex, cross-domain, and politically consequential (Walker-Munro and Bachmann, 2026).

The argument is that not all states in Southeastern Europe should adopt the same counterintelligence model. Institutional design must take into account constitutional traditions, threat profiles, administrative capacity, and historical experience. The central argument, rather, is that counterintelligence should be raised from a scattered operational function to a coherent strategic capability. In an age of hybrid threats, foreign information manipulation and interference, cyber-espionage, covert influence and geopolitical competition, counterintelligence is no longer limited to the detection of espionage (Drew, 2026). It is also contributing to protecting the integrity of democratic institutions, the security of decision-making, the resilience of critical infrastructure, and the sovereignty of the state (Kanellopoulos and Ioannidis, 2023).

Hybrid threats provide the broader strategic context for this analysis, but they should not be treated as synonymous with counterintelligence. Hybrid activity may combine military and non-military, overt and covert instruments, including cyber operations, disinformation, economic pressure, proxy actors and conventional force. Counterintelligence addresses the narrower question of whether such activities involve hostile intelligence direction, clandestine collection, covert access, agent recruitment, deception, penetration, sabotage or concealed foreign influence.

This distinction is important because many harmful activities fall primarily within the responsibilities of law enforcement, cybersecurity authorities, financial regulators, electoral bodies or strategic-communications institutions. A cyberattack, misleading narrative or suspicious investment does not automatically constitute a counterintelligence case. It becomes relevant to counterintelligence when credible indicators connect the activity to hostile foreign intelligence objectives, covert state direction, clandestine access or the exploitation of protected institutions and decision-making processes.

Foreign information manipulation and interference illustrates this overlap. The European External Action Service has identified it as an increasing security and foreign-policy challenge for the European Union and its partners. Counterintelligence institutions may contribute where information operations involve covert state sponsorship, concealed intermediaries, clandestine financing, intelligence-service direction or attempts to recruit and manipulate influential individuals. They should not, however, acquire general responsibility for regulating public debate or determining the truthfulness of lawful political expression. This boundary is necessary to protect freedom of expression and to prevent counterintelligence mandates from expanding into political or ideological surveillance.

The changing threat environment in Southeastern Europe

The eight states examined in this article occupy overlapping but distinct security environments. Greece and Bulgaria are members of both the European Union and the North Atlantic Treaty Organization, whereas Albania, Montenegro and North Macedonia are members of NATO but remain candidates for EU membership. Serbia maintains military neutrality, Bosnia and Herzegovina operates within a highly decentralised constitutional system, and Kosovo's international status and security architecture remain contested. These differences shape the legal authority, institutional capacity, international partnerships and political constraints under which national counterintelligence functions operate. The region should therefore not be understood as a homogeneous security space. Nevertheless, the eight states are connected by cross-border infrastructure, economic relationships, organised crime networks, political disputes, media environments and competing external influences. Their vulnerabilities also differ in degree and form. Some face pronounced cyber and critical-infrastructure risks; others confront problems involving political interference, institutional capture, classified-information security, strategic corruption or the exploitation of unresolved constitutional and identity disputes. The analytical value of considering them together lies in comparing how different institutional systems respond to partly interconnected threats, rather than in assuming that every state faces the same threat profile. This combination of interconnected external pressures and uneven domestic institutional development also reflects, in a limited sense, the International Relations insight associated with uneven and combined development: political units may interact within the same international environment while remaining institutionally dissimilar and developing under different historical conditions. The concept is used here only to emphasise the analytical significance of unevenness and interaction, rather than as a comprehensive theoretical framework for the article (Rosenberg, 2010).

Traditional or "classical" espionage refers here to clandestine efforts to obtain protected political, military, diplomatic, technological or economic information through recruited human sources, covert access, undeclared intelligence officers, technical collection or the exploitation of insiders. These activities remain an important counterintelligence concern, particularly where foreign actors seek access to defence planning, diplomatic decision-making, critical infrastructure, emerging technologies or classified information. Such espionage is not unique to Southeastern Europe and many of its techniques are also observed elsewhere in Europe. The regional issue is therefore not the existence of an entirely distinct form of espionage. Rather, the significance of traditional espionage may be increased by the interaction between foreign intelligence activity and uneven institutional capacity, political polarisation, corruption risks, unresolved interstate disputes and differences in democratic oversight. Traditional intelligence collection must also be considered alongside cyber-enabled espionage, covert influence, illicit political or economic

relationships, information manipulation and the use of intermediaries or proxy networks. These activities may be operationally separate, but they can serve mutually reinforcing strategic objectives (Tekorius,2026).

Publicly documented cases illustrate why the threat environment should be analysed through distinct national contexts. In Albania, the malicious cyber activities of July 2022 directly targeted critical infrastructure and disrupted the provision of public services. The European Union characterised the incident as an attempt to threaten Albania's security and undermine democratic institutions, demonstrating how a cyber operation may have consequences extending beyond a technical information-security breach (Council of the European Union, 2022).

Bulgaria provides a different illustration centred on traditional espionage and insider access. In November 2021, the Sofia Military District Prosecutor's Office filed an indictment against six individuals accused of forming an espionage group and collecting classified information for a foreign state. According to the Prosecutor's Office, members of the alleged group occupied positions providing access to Bulgarian, NATO and European Union classified information. The case demonstrates the continuing relevance of human recruitment, insider threats and the protection of classified defence information within a contemporary Euro-Atlantic security environment (Prosecutor's Office of the Republic of Bulgaria, 2021). These examples should not be interpreted as evidence that Albania and Bulgaria face identical threats or that the same institutional response would be appropriate in both states. Instead, they demonstrate the breadth of activities that may require counterintelligence attention and the need to adapt institutional arrangements to national threat profiles.

The Western Balkans are a case in point of many of these dynamics. According to a 2024 report by the EU Institute for Security Studies (2024), there is a need to strengthen the regional response to these threats. The same report said that the region saw a steep increase in cyber-enabled attacks during 2020-2024. Such attacks should not be seen as simply technical cyber-security incidents (Sithole and Du Toit, 2002). They may also be used for intelligence purposes: mapping institutional weaknesses, gaining access to sensitive data, undermining public trust, coercing governments or preparing future influence operations (Barnea, 2019).

Moreover. foreign information manipulation and interference further complicate the picture. In its 2025 report on FIMI threats, the EEAS described foreign actors who use digital infrastructure to manipulate and interfere in the information space of the EU and partner countries, including activity attributed mainly to Russia but also to China. FIMI, in its annual report for 2026, said it had passed a new level of operational complexity and global reach in 2025 (EEAS, 2025; 2026a). These trends illustrate that the information domain has become a key arena of strategic competition.

Eventually, the implication for Southeastern Europe is clear: counterintelligence must be understood as a cross-domain discipline. It has to deal with not just hostile officers and recruited agents, but also influence infrastructures, cyber intrusions, insider threats, front organisations, covert funding channels, proxy networks and vulnerabilities in critical decision-making systems.

The examples and threat categories discussed above do not suggest that counterintelligence should absorb every function associated with hybrid-threat response. Rather, they demonstrate the need for counterintelligence bodies to recognise when activities observed by other institutions form part of a covert foreign intelligence campaign. The strategic challenge is therefore one of attribution, integration and coordination: technical, financial, political and human indicators may acquire counterintelligence significance only when they are assessed together and connected to hostile intent.

Counterintelligence as a strategic state function

For the purposes of this article, counterintelligence is defined as the organised identification, assessment, prevention, exploitation and disruption of intelligence activities conducted by hostile foreign states, their intelligence services, intermediaries or proxies against a state's institutions, personnel, information, infrastructure and decision-making processes. Its traditional core remains the protection of the state against espionage, penetration, recruitment, deception, sabotage and insider threats. Contemporary counterintelligence, however, also requires attention to cyber-enabled intelligence collection, covert influence, strategic corruption, illicit access to sensitive technologies and attempts to manipulate political or institutional processes (Prunckun, 2019; Kanellopoulos, 2022; Putter and Bachmann, 2022).

This article analyses counterintelligence primarily at the national strategic and institutional levels. It does not attempt to evaluate individual operations, classified capabilities or the tactical performance of particular officers and units. The term therefore encompasses the civilian, military, police, cyber, financial and regulatory institutions that contribute to identifying and countering hostile foreign intelligence activity. Where the article refers more generally to "intelligence", it does so only in relation to the wider national intelligence structures within which counterintelligence responsibilities are located.

Under this definition, counterintelligence is both a specialised intelligence discipline and a strategic function of the state. Operational counterintelligence activities may be conducted by particular civilian, military or law-enforcement bodies, but their effectiveness depends on national-level arrangements for assessment, coordination, legal authority, information sharing and democratic oversight. Counterintelligence contributes to national sovereignty by protecting the independence and integrity of state decision-making from covert foreign interference. It also supports democratic resilience by identifying attempts to penetrate public institutions, distort political processes, compromise sensitive information or exploit strategic sectors (Putter and Bachmann, 2022). Furthermore, it safeguards strategic sectors, intellectual property, defence industries, ports, energy systems, telecommunications and emerging technologies, promoting economic security and supporting cybersecurity by linking technical intrusions to hostile intelligence intent and larger strategic campaigns (Prunckun, 2019).

Describing counterintelligence as a strategic state function does not mean that a single institution should control all security activity associated with foreign interference. It means that the state requires the capacity to combine relevant information, assess hostile intent, identify vulnerabilities, assign responsibilities and provide warning to authorised decision-makers. Operational authority may remain distributed among intelligence services, police bodies, military institutions, cybersecurity agencies, financial-intelligence units and regulators.

Three analytical functions are particularly important. The first is threat assessment. Counterintelligence analysis must distinguish between ordinary diplomatic, commercial, political or cultural activity and conduct that involves concealed direction, clandestine access, prohibited intelligence collection or coercive foreign influence. This requires evidence-based assessment and clear legal thresholds, not assumptions based solely on nationality, political opinion or contact with foreign actors.

The second function is vulnerability assessment. Counterintelligence should examine not only what hostile actors are attempting to do, but also which institutional conditions permit exploitation. These may include inadequate personnel vetting, weak information security, unclear

reporting obligations, corruption risks, insecure procurement, insufficient protection of classified information or limited awareness among public officials and strategic industries. A strategic approach therefore combines investigation of hostile activity with preventive work designed to reduce opportunities for penetration and manipulation.

The third function is strategic warning. Individual agencies may observe separate indicators without recognising their combined significance. A cyber authority may identify unauthorised access, a financial-intelligence unit may detect an opaque transfer, and a security service may record suspicious contact with an official. None of these indicators necessarily proves hostile intelligence activity in isolation. A national counterintelligence capacity should provide a lawful mechanism through which such information can be assessed jointly, while preserving statutory limits, evidentiary standards and controls on the dissemination of personal data.

Counterintelligence also has an advisory function. Strategic assessments may inform decisions concerning the protection of classified information, critical infrastructure, research partnerships, foreign investment, electoral security and public-sector integrity. The counterintelligence contribution should be limited to identifying covert foreign intelligence risks. Final policy decisions should remain with the legally responsible ministries, regulators, courts or elected authorities. This separation reduces the danger that a security service becomes an unaccountable decision-maker in areas extending beyond its mandate.

The strategic value of counterintelligence therefore depends on its capacity to connect operational findings with broader patterns without erasing institutional boundaries. Excessive fragmentation may prevent the state from identifying a coordinated campaign, but excessive concentration may weaken specialisation, legal safeguards and democratic control. The appropriate objective is structured integration: clearly allocated responsibilities, secure information exchange, joint assessment where necessary and independent oversight of the institutions involved.

Ultimately, this is why counterintelligence should not be treated as an uncoordinated subsidiary responsibility within larger security bureaucracies. In a disjointed counterintelligence environment, the state might know about particular incidents but not about trends. One agency may see a cyber intrusion. Another may see suspicious political financing or disinformation activity. Another may see a contact between a foreign official and a sensitive public servant. Without an institutional mechanism to bring them together, the state may lose the intelligence architecture that links these indicators (Mobley and Wege, 2021).

The challenge is therefore both institutional and analytical. The eight states require arrangements capable of producing national-level assessments, coordinating lawful defensive measures and advising political authorities without centralising all operational powers in one organisation. “Institutional ownership” should mean that a clearly identified body is responsible for strategic integration and warning. It should not mean that the lead institution automatically acquires the powers or responsibilities of the police, armed forces, cybersecurity authorities, prosecutors, financial regulators or independent oversight bodies.

Existing national arrangements: variation rather than institutional absence. Publicly available legal and institutional material does not support a general claim that the eight states examined in this article lack counterintelligence laws, organisations or assigned responsibilities. Each state has established institutions authorised to address espionage, hostile intelligence activity, threats to the constitutional order or related national-security concerns. The principal differences concern where those responsibilities are located, how broadly they are defined, how civilian and military functions are divided, and what mechanisms exist for coordination and oversight.

Fragmentation should therefore be treated as an empirical question to be assessed within each national system rather than assumed to be a uniform regional condition.

In Greece, the National Intelligence Service is the principal civilian intelligence institution. Its publicly stated objective includes preventing, deterring and neutralising espionage and terrorist threats. Relevant responsibilities are nevertheless distributed across a wider institutional environment. The National Intelligence Service addresses intelligence and counterintelligence threats, while the National Cybersecurity Authority performs regulatory, supervisory and coordinating functions in cybersecurity, including responsibility for national strategy and incident-response arrangements. Greece therefore illustrates a system in which counterintelligence and cybersecurity have distinct institutional centres. The analytical issue is not the absence of responsible organisations, but whether information derived from espionage investigations, cyber incidents, critical-infrastructure protection and other relevant domains can be integrated into a coherent national assessment (National Intelligence Service, 2026)

Albania also possesses established civilian and military counterintelligence structures. The State Intelligence Service operates under Law No. 8391 of 1998 and is authorised to obtain intelligence and counterintelligence information relevant to national security. Its stated responsibilities include counterintelligence activity intended to protect the state's integrity, independence and constitutional order. Within the defence sector, the Defence Intelligence and Security Agency provides intelligence, counterintelligence and security support to the Ministry of Defence and the Albanian Armed Forces. Albania consequently represents a divided but legally constituted model in which civilian and military institutions possess related responsibilities. Any assessment of fragmentation must examine the effectiveness of coordination between these bodies rather than infer institutional absence from the existence of multiple services (State Intelligence Service of Albania, 2026)

North Macedonia established the Agency for National Security in 2019 as an independent state-administration body, replacing the former Security and Counterintelligence Directorate located within the Ministry of the Interior. The Agency's stated responsibilities include preventing and detecting espionage, monitoring national-security risks and exchanging information with domestic and foreign partners. This institutional change is particularly relevant because it followed the surveillance and governance failures discussed above. North Macedonia therefore demonstrates that counterintelligence reform may involve restructuring an existing service, separating it from a ministry and revising oversight arrangements rather than establishing counterintelligence capacity for the first time (Agency for National Security of the Republic of North Macedonia, 2026).

Montenegro's National Security Agency is a civilian security-intelligence service within the national security system. Montenegro has also adopted a broader statutory framework for coordinating the intelligence and security sector, including national-level and operational coordinating mechanisms. This model is significant because it separates the existence of a principal security-intelligence service from the separate problem of inter-agency coordination. Montenegro's experience suggests that reform may focus on interoperability, lawful information exchange and oversight of existing bodies instead of creating an additional operational agency (Government of Montenegro, 2014).

Kosovo's institutional framework is comparatively explicit in its use of the term counterintelligence. The Law on the Kosovo Intelligence Agency established the Agency to collect, analyse and disseminate intelligence concerning intelligence, counterintelligence, domestic and foreign threats, terrorism, organised crime, sabotage and other matters affecting

Kosovo's security. The legislation therefore demonstrates that a formal counterintelligence mandate already exists. The relevant questions for this article concern the scope of that mandate, its relationship with police and defence institutions, and the adequacy of coordination and democratic supervision rather than whether Kosovo possesses a counterintelligence organisation (Kosovo Intelligence Agency, 2008).

Serbia combines a civilian national security service with a separate military counterintelligence institution. The Security Information Agency is a civilian national security service responsible for protecting the security and constitutional order of Serbia and for collecting and assessing security-intelligence information. The Military Security Agency provides security and counterintelligence protection to the Ministry of Defence and the Serbian Armed Forces. Serbia therefore offers a clear example of functionally differentiated civilian and military responsibilities. Such differentiation is not necessarily a weakness, but it creates a requirement for clear jurisdictional boundaries, lawful exchange of information and effective national coordination where threats cross civilian, defence, cyber and political domains (Security Information Agency, 2026)

Bosnia and Herzegovina possess a state-level civilian Intelligence and Security Agency with jurisdiction throughout the country. The 2004 law establishing the Agency authorises it to collect, analyse and disseminate intelligence concerning threats to sovereignty, territorial integrity, the constitutional order and fundamental economic stability. The statutory definition of security threats expressly includes espionage and sabotage. Bosnia and Herzegovina's complex constitutional structure therefore does not mean that civilian counterintelligence responsibility is legally absent. Its system instead raises questions about how a state-level intelligence body cooperates with law-enforcement, prosecutorial, defence and entity-level institutions within a highly decentralised political structure (Intelligence and Security Agency of Bosnia and Herzegovina, 2004).

Bulgaria separates domestic counterintelligence and security responsibilities from foreign intelligence collection. The State Agency for National Security is designated as a specialised counterintelligence and security body responsible for detecting, preventing and neutralising threats to national security. The State Intelligence Agency, by contrast, is responsible principally for obtaining and analysing foreign intelligence concerning external threats. Bulgaria thus provides an example of a more functionally differentiated intelligence architecture. As in Serbia, the existence of separate organisations is not itself evidence of dysfunctional fragmentation. The appropriate analytical question is whether their mandates, reporting relationships, information-sharing procedures and oversight arrangements enable them to respond coherently to threats that cross domestic and external domain (State Agency for National Security of Bulgaria, 2026)

This comparison identifies at least three broad institutional patterns: systems centred on a civilian service with an extensive national-security mandate; systems that distribute responsibilities between civilian and military services; and systems that supplement existing services with statutory coordination mechanisms. These categories overlap, and none constitutes an automatically preferable model. Institutional plurality may preserve specialist expertise and legal boundaries, whereas excessive concentration may create risks of politicisation or insufficient oversight. Conversely, poorly coordinated plurality may prevent institutions from combining indicators held by different agencies. The central concern of this article is therefore not that counterintelligence is absent across Southeastern Europe. It is that the existence of statutory mandates does not by itself establish strategic coherence, operational effectiveness or democratic legitimacy. Determining whether fragmentation constitutes a significant weakness requires

country-specific examination of mandates, information-sharing practices, analytical structures, oversight arrangements and documented institutional failures.

Fragmentation carries several risks. First, it undermines the early warning. Hostile intelligence operations are seldom perfect from the outset. They appear in small signals across domains: strange contacts, cyber probing, unexplained financial flows, narrative amplification, procurement irregularities, access attempts or insider cultivation. Each institution might only see its own piece, and the larger pattern might be invisible (George, 2019). Second, fragmentation breeds reactive responses. States may react after cyberattacks, leaks, scandals or controversies over foreign interference have already taken place. An effective counterintelligence system must detect vulnerabilities before they are exploited, and provide strategic warning of hostile activity before political damage is done.

Third, fragmentation creates ambiguity about the mandate. Agencies can disclaim responsibility when threats don't fit traditional categories. Cyber-enabled influence operations, strategic corruption or foreign-linked organised-crime facilitation may fall between intelligence, law enforcement, anti-corruption and cyber-security mandates (Gentry, 2022). Fourth, fragmentation may undermine democratic accountability. With several agencies performing partial counterintelligence functions, oversight bodies can struggle to ascertain who is responsible, what legal standards apply and how intrusive measures are authorised. If properly designed, a dedicated or clearly empowered counterintelligence institution can make responsibility more visible and oversight more effective (Kniep et al., 2023).

Finally, fragmentation hinders international cooperation. They are more likely to share sensitive intelligence with foreign partners if they know which institution is responsible, legally authorised, professionally competent and secure. In areas where the threat from across the border is high, trusted liaison arrangements are essential.

Institutional integration and the conditional case for dedicated capacity

The need for strategic integration does not imply that counterintelligence should be organisationally separated from other intelligence and security functions. Counterintelligence may be embedded across existing civilian, military and law-enforcement institutions, provided that responsibilities are clearly allocated, relevant information can be exchanged lawfully and a mechanism exists for national-level assessment and strategic warning. In other national systems, a dedicated directorate, coordinating centre or, in more limited circumstances, a separate agency may provide clearer institutional ownership, specialist expertise and accountability. The relevant question is therefore not whether counterintelligence is organisationally separate, but whether the national system can integrate threat information, preserve specialist tradecraft, coordinate appropriate responses and assign responsibility for strategic warning and oversight (Moyers, 2025).Where national conditions justify a dedicated coordinating body or agency, it can serve as a national focal point for the identification and assessment of hostile intelligence activity. It can include information from security services, police, military bodies, cyber authorities, border agencies, financial intelligence units, anti-corruption institutions, electoral bodies and critical-infrastructure regulators. It is able to retain an image of the national threat and advise political decision makers on the risks to sovereignty and institutional integrity. It can also develop specialist trade craft. Counterintelligence needs its own professional culture. This includes detection of deception, hostile recruitment, surveillance, clandestine networks, covert access, insider threats, technical compromise, front organisations and influence infrastructures. These are not routine criminal investigations, routine intelligence collection, or military threat assessment.

A clearly designated counterintelligence function, whether embedded within an existing service or organised separately, can also improve prevention. A modern counterintelligence service must not only investigate hostile actions after they have taken place. It should conduct vulnerability assessments, security education, insider-threat programmes, liaise with critical sectors, protect sensitive research and give defensive briefings to public officials, political parties, academia, technology companies and strategic industries.

The democratic argument for institutional clarity is conditional rather than automatic. A dedicated or clearly empowered institution may make responsibility more visible, but institutional concentration can also increase the risks associated with secrecy, intrusive powers and political control. Democratic legitimacy therefore depends less on the organisational title of the responsible body than on the relationship between mandate, authority and accountability. Counterintelligence responsibilities should be established in accessible legislation, intrusive measures should require independent authorisation, executive direction should be separated from operational decision-making, and parliamentary and independent bodies should possess the authority and expertise necessary to identify misuse. Institutionalisation should consequently mean both clearer operational responsibility and stronger democratic control, not the creation of unchecked security power.

Differentiated and sequenced policy pathways for Southeastern Europe

Counterintelligence reform in the eight states examined should be differentiated, proportionate and sequenced. The appropriate objective is not necessarily the creation of a new organisation, but the development of a coherent national capacity with identifiable leadership, lawful authority, effective coordination and democratic accountability. Institutional solutions must reflect the scale of the threat, the maturity of existing services, constitutional arrangements, available resources and the capacity of oversight institutions. A reform process should begin with a national counterintelligence review rather than with a predetermined organisational model. This review should map existing statutory mandates, identify duplication and gaps, assess mechanisms for information sharing, examine the adequacy of oversight and determine whether relevant institutions possess the necessary analytical, linguistic, cyber, financial and legal expertise. It should also identify which reforms can be achieved by reallocating existing responsibilities and which require additional personnel or expenditure.

Three broad institutional pathways are available. First, a state with a capable domestic intelligence service and a sufficiently clear legal mandate may strengthen the counterintelligence directorate within that service. Secondly, a state in which relevant expertise is distributed across several competent bodies may establish a national coordination centre or a statutory inter-agency mechanism. Thirdly, the creation of a separate counterintelligence agency may be justified where no existing body can provide institutional leadership and where the expected benefits outweigh the financial, administrative and democratic risks of creating an additional security organisation. These pathways are alternatives rather than cumulative requirements.

1. Select an institutional model through national assessment

Each state should assess whether its existing institutional structure provides clear leadership for strategic counterintelligence. The assessment should distinguish between operational responsibilities and national coordination. Several agencies may continue to conduct specialised counterintelligence activities, provided that statutory responsibility exists for integrating threat

assessments, resolving jurisdictional disputes and advising national decision-makers. Where an existing civilian or domestic intelligence service possesses an appropriate mandate, professional capacity and credible oversight, strengthening that institution may be less costly and less disruptive than creating a new agency. Reform could include establishing a dedicated counterintelligence directorate, improving analytical capacity, clarifying information-sharing obligations and assigning responsibility for producing national counterintelligence assessments. Moreover, where responsibilities are divided among intelligence, military, police, cyber, financial and regulatory bodies, a national counterintelligence centre or permanent inter-agency mechanism may be more appropriate. Such a centre need not possess independent operational powers. It may instead provide joint analysis, strategic warning, vulnerability assessment, coordination and policy advice while operational authority remains with existing institutions. A separate counterintelligence agency should be considered only where existing arrangements are persistently incapable of providing leadership, coordination and professional specialisation. Before establishing a new body, the government should demonstrate that its mandate will not duplicate existing functions, that sustainable funding is available and that parliamentary, judicial and independent oversight bodies possess the capacity to supervise it effectively.

2. Provide an accurate legal definition for counterintelligence

Counterintelligence reform must initiate with a legal definition. The law should specify its mission, powers, limits, oversight mechanisms, and relationship to other agencies. The mandate should focus on foreign intelligence threats, espionage, sabotage, hostile influence, cyber-enabled penetration, insider threats, and threats to constitutional order involving foreign actors. Counterintelligence is close to politically sensitive areas and legal clarity is important. Without clear boundaries it can be conflated with public-order policing or political surveillance or ideological monitoring. Democratic counter-intelligence should protect constitutional institutions from hostile foreign activity, not police lawful dissent.

3. Embed counterintelligence reform within democratic security-sector governance

Counterintelligence reform should be understood as part of the wider democratic governance of the security sector rather than as a narrowly organisational exercise. The literature on post-communist and Western Balkan security reform demonstrates that formal civilian authority does not by itself guarantee democratic control. Effective governance also depends on clearly allocated legal responsibilities, professional civilian expertise, institutional accountability, transparency compatible with legitimate secrecy and the capacity to investigate misconduct (Edmunds, 2001; Bellamy and Edmunds, 2005; Edmunds, 2007).

This distinction is important because political control and democratic control are not equivalent. A service may be closely controlled by the executive while remaining weakly accountable to parliament, the courts, independent regulators and the public. Excessive executive control may facilitate politicisation, whereas weak executive direction may permit institutional autonomy without adequate accountability. Democratic governance therefore requires a distribution of responsibilities across several institutions rather than dependence on a single supervising authority.

The executive should establish lawful national priorities, ensure coordination among responsible bodies and maintain internal systems for compliance and financial control. It should not direct investigations for partisan purposes or determine operational conclusions. Parliamentary

committees should examine legislation, policy, expenditure, institutional performance and compliance, but should not attempt to manage individual operations. Courts or other legally authorised bodies should provide independent authorisation and review of intrusive measures. Data-protection authorities, inspectors-general, ombuds institutions and specialised review bodies should be empowered to examine areas falling within their respective mandates.

Oversight must also be substantive rather than merely formal. Parliamentary committees and independent review bodies require appropriate security clearances, access to relevant classified information, specialist staff, technical expertise and adequate financial resources. Without these capacities, the existence of an oversight body may provide an appearance of accountability without enabling meaningful scrutiny. Oversight institutions should be able to examine the legality, necessity and proportionality of intrusive measures; review information-sharing and data-retention practices; investigate complaints; inspect budgets and procurement; and report findings in a form compatible with national-security requirements (Born and Caparini, 2007; DCAF, 2017).

The broader literature on post-communist civil–military relations also cautions against treating democratic reform as a single institutional event. Reform is an extended political and organisational process shaped by historical legacies, professional cultures, competing institutional interests, levels of civilian expertise and external incentives (Cottey, Edmunds and Forster, 2005; Bellamy and Edmunds, 2005; Edmunds, 2007). Applied to counterintelligence, this means that adopting legislation or creating a parliamentary committee is only an initial step. Democratic control must be reinforced through sustained professionalisation, periodic legal review, institutional learning and credible enforcement when officials exceed their authority.

The suitability of specific oversight arrangements will vary among the eight states. Constitutional structures, judicial systems and parliamentary practices differ, and Bosnia and Herzegovina's decentralised governance presents different challenges from the more centralised systems found elsewhere in the study. Nevertheless, the underlying principle remains consistent: any expansion of counterintelligence authority must be accompanied by an equivalent expansion in the capacity to authorise, inspect, contest and remedy its use.

4. Combine cyber, economic and information-domain counterintelligence

Counterintelligence institutions must be shaped for the current threat environment. Cyber operations, economic penetration, critical-infrastructure targeting, technology acquisition, illicit finance, and information manipulation should not be divorced from counterintelligence. They are often the mechanisms hostile intelligence services operate through (Ioannidis and Kanellopoulos, 2025).

This calls for formal cooperation with cyber-security agencies, national computer emergency response teams, financial intelligence units, anti-corruption bodies, procurement authorities, investment-screening mechanisms, electoral commissions and critical-infrastructure regulators. Consequently, a modern counterintelligence organization should have analytical components that can link technical cyber indicators to geopolitical intent, illicit finance to influence operations, and information manipulation to hostile intelligence objectives.

5. Protect vital infrastructure and strategic sectors

The states should integrate counterintelligence into the protection of critical infrastructure and strategic sectors. Potential targets include energy systems, ports, telecommunications networks, transport corridors, defence industries, research institutions, public-health systems, financial infrastructure and digital platforms. Likewise, counterintelligence agencies should be

offering threat briefings, security guidance, and vulnerability assessments to both public and private actors. They should also improve investment-screening procedures, security of supply chains, policies on research security, and the mitigation of insider threats (Kanellopoulos, 2022). This has to be done carefully, with respect to academic freedom, market openness and civil liberties. The aim is not to securitise society but to protect strategic assets from clandestine foreign exploitation.

6. Improve regional and, where appropriate, Euro-Atlantic cooperation

Hostile intelligence activity does not respect borders. States should therefore strengthen cross-border intelligence liaison, information-sharing, joint training and other forms of practical cooperation in ways consistent with their foreign-policy alignments, legal obligations and national security strategies. For European Union and NATO members and partners, Euro-Atlantic mechanisms may provide established channels for training, exercises, technical assistance and access to specialist capabilities. States whose strategic alignment differs from these frameworks may rely more heavily on bilateral, regional or other compatible arrangements. The relevant principle is functional cooperation against cross-border threats, rather than an assumption that all eight states share an identical geopolitical orientation.

7. Sequence reform according to resources and institutional capacity

Resource limitations require prioritisation rather than the abandonment of reform. States with constrained budgets should initially concentrate on measures that improve the use of existing capacity. These may include clarifying mandates, appointing a lead coordinating authority, establishing secure information-sharing procedures, conducting joint threat assessments and providing targeted training to personnel already working in intelligence, policing, cybersecurity, financial investigation and critical-infrastructure protection.

More resource-intensive reforms should be implemented in phases. The first phase should address legal definitions, institutional responsibilities, oversight authority and inter-agency procedures. The second should develop specialist analytical teams, secure information systems, training programmes and liaison arrangements with critical sectors. A third phase may introduce more advanced technical capabilities, regional training platforms and specialised units where national assessments demonstrate a continuing operational need.

Regional cooperation and, where compatible with national strategic alignment, Euro-Atlantic cooperation can reduce costs through joint training, shared exercises, technical assistance and access to established standards. Such cooperation cannot replace national responsibility or justify dependence on foreign services, but it can help smaller administrations develop specialist skills that would be expensive to maintain independently. Governments should also subject proposed reforms to multi-year financial planning so that institutions are not created without the personnel, technology and oversight resources necessary to operate lawfully and effectively.

The feasibility of democratic reform must also be evaluated. Where parliamentary committees, courts, data-protection authorities or independent inspectors lack the expertise and resources to supervise expanded counterintelligence powers, operational expansion should not precede oversight reform. In such circumstances, strengthening supervisory capacity is a substantive component of counterintelligence reform rather than a secondary institutional consideration.

Risks and safeguards

The institutionalisation of counterintelligence carries significant democratic risks. These risks are particularly important where intelligence bodies have previously been affected by political control, weak oversight, opaque surveillance procedures or limited access to effective remedies. Reform must therefore strengthen both operational capability and the institutions responsible for authorising, reviewing and investigating counterintelligence activity.

The first risk is mandate expansion. A counterintelligence institution may interpret threats so broadly that lawful political activity, journalism, civil-society advocacy or minority representation becomes subject to surveillance. Counterintelligence mandates should consequently be tied to clearly defined conduct involving hostile foreign intelligence activity, espionage, sabotage, covert foreign direction or other legally specified threats. Political disagreement, criticism of the government, contact with foreign organisations or participation in lawful protest should not, by themselves, constitute counterintelligence grounds. The second risk is politicisation and the misuse of surveillance powers. The experience of North Macedonia demonstrates how the concentration of technical and institutional power can facilitate systemic abuse. The 2015 interception scandal reportedly involved approximately 670,000 illegally recorded conversations associated with more than 20,000 telephone numbers. A Council of Europe Parliamentary Assembly report, referring to the findings of the European Union's senior expert group, stated that the national security services had been misused to monitor public officials, prosecutors, judges and political opponents. The subsequent reform process separated certain technical interception functions and introduced additional judicial, parliamentary and civilian oversight mechanisms (Parliamentary Assembly of the Council of Europe, 2019).

Moreover, Greece provides a more recent illustration of the challenges created by overlapping intelligence surveillance and commercial spyware. The European Parliament reported that a Greek Member of the European Parliament and a journalist had been subjected to lawful interception by the Hellenic National Intelligence Service and had also been targeted with Predator spyware. Although the Greek Government denied purchasing or using Predator, the case generated serious concerns regarding authorisation, notification, independent investigation and the relationship between state surveillance and private surveillance technologies (European Parliament, 2023).

The third risk is duplication. The creation of a new institution with undefined mandates might result in greater fragmentation. Therefore, reform has to cover inter-agency protocols, rules of information sharing, deconfliction mechanisms and clear responsibility for strategic assessment. The fourth risk is excessive secrecy. Counterintelligence operations require confidentiality, but secrecy should not prevent institutional accountability. Oversight bodies must have the legal authority, appropriate security clearances, technical expertise and resources required to examine classified activity. They should be able to inspect surveillance authorisations, access operational records, review data-retention practices, investigate complaints and refer suspected illegality for prosecution or judicial review. Counterintelligence bodies should also publish appropriately redacted annual reports, aggregate surveillance statistics, descriptions of their statutory responsibilities and general threat assessments. Such transparency can increase public confidence without exposing operational methods or sensitive sources.

Lastly, the fifth risk is lack of capacity. Just naming an agency does not solve the problem. Effective counterintelligence requires trained personnel, secure information systems, analytical capability, legal expertise, language skills, cyber competence, financial investigation knowledge and sustained political support.

Implications and Conclusions

This article has examined counterintelligence arrangements and reform challenges across Greece, Albania, North Macedonia, Montenegro, Kosovo, Serbia, Bosnia and Herzegovina, and Bulgaria. The comparison does not support the proposition that counterintelligence functions or legal mandates are absent across the region. All eight states possess institutions with responsibilities relating to espionage, hostile intelligence activity, national security or the protection of the constitutional order. However, these responsibilities are distributed differently, and the existence of a formal mandate does not necessarily ensure strategic integration, operational effectiveness or democratic legitimacy.

The cases considered also demonstrate that the term "regional threat environment" conceals significant national variation. Albania and Montenegro have experienced disruptive cyber incidents affecting government systems and public functions. Bulgaria illustrates the continuing importance of alleged human recruitment and insider access to classified information. North Macedonia and Greece demonstrate the democratic risks associated with intrusive surveillance and inadequate accountability. Serbia raises questions concerning the legal boundary between intelligence activity and criminal investigation, while Bosnia and Herzegovina illustrates how constitutional and political fragmentation can inhibit coordinated policy. Kosovo demonstrates that formal oversight provisions require sufficient parliamentary and institutional capacity to operate effectively. The comparative value of the eight cases therefore lies in variation rather than uniformity. They do not support a shared regional diagnosis in the sense that every state possesses the same institutional weakness. Instead, they reveal a common decision problem at a higher level of analysis: how national authorities should determine whether greater counterintelligence coherence is best achieved through stronger capacity within an existing service, improved coordination among several institutions, or a new organisational structure. The comparison is intended to identify the conditions under which these alternatives may be appropriate, not to flatten national differences into a single regional model.

These differences have two principal implications. First, counterintelligence reform should begin with a national review of threats, mandates, coordination arrangements, resources and oversight capacity. Institutional fragmentation should be demonstrated through evidence rather than assumed from the existence of several responsible bodies. Multiple institutions may provide valuable specialisation where their mandates are clear and information can be exchanged lawfully. Conversely, creating a new organisation may increase duplication or concentrate intrusive powers without resolving underlying problems.

Secondly, institutional effectiveness and democratic accountability should be treated as mutually dependent rather than competing objectives. A counterintelligence system that lacks lawful authority, professional independence and credible oversight may itself create vulnerabilities through politicisation, unlawful surveillance or loss of public trust. Equally, oversight that exists only formally, without access to classified information, technical expertise or investigatory authority, cannot provide meaningful democratic control. Expansion of counterintelligence capability should therefore proceed alongside the development of parliamentary, judicial and independent supervisory capacity.

The appropriate institutional pathway will differ by country. Some states may benefit from strengthening a counterintelligence directorate within an existing civilian service. Others may require a statutory coordinating mechanism capable of integrating information held by civilian, military, police, cyber, financial and regulatory institutions. A separate agency may be appropriate only where existing arrangements cannot provide clear leadership and where sustainable resources

and effective oversight can be demonstrated. In resource-constrained systems, legal clarification, joint assessments, secure information-sharing procedures and targeted specialist training may offer more immediate benefits than large-scale institutional restructuring.

The article is necessarily limited by its reliance on publicly available material. It does not evaluate classified operations, undisclosed capabilities or the performance of individual services. The cases are illustrative rather than statistically representative, and further country-level research is required to assess how statutory mandates operate in practice. Interviews with former officials, oversight bodies, policymakers, journalists and civil-society organisations could provide a stronger basis for evaluating institutional effectiveness and democratic accountability.

The central conclusion is therefore comparative rather than regionally prescriptive. Counterintelligence should be developed as a coherent strategic capability, but coherence does not require organisational uniformity, institutional separation or centralisation. Across the eight cases, the relevant policy task is to identify whether the principal national constraint lies in mandate, coordination, analytical capacity, resources or democratic oversight and then to select the least disruptive institutional pathway capable of addressing that constraint. Where an existing service possesses the necessary mandate, capacity and credible oversight, strengthening that service may be preferable. Where competent functions are distributed across several institutions but strategic integration is weak, a statutory coordinating mechanism may be more appropriate. A separate agency should be considered only where existing arrangements cannot provide effective leadership and where the necessary resources and oversight capacity can be sustained. The value of the eight-country comparison lies precisely in demonstrating why a common strategic objective can require different national institutional responses.

References

3rd EEAS Report on Foreign Information Manipulation and Interference Threats. (2025, March 19). EEAS. https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en?utm_source=chatgpt.com

Agency for National Security of the Republic of North Macedonia (2026). Mission and Vision of ANB. https://anb.gov.mk/en/za-anb/

Barnea, A. (2019). Big data and counterintelligence in Western countries. *International Journal of Intelligence and CounterIntelligence*, *32*(3), 433–447. https://doi.org/10.1080/08850607.2019.1605804

Bellamy, A. J., & Edmunds, T. (2005). Civil–military relations in Croatia: Politicisation and politics of reform. European Security, 14(1), 71–93. https://doi.org/10.1080/09662830500042338

Born, H., & Caparini, M. (Eds.). (2007). Democratic control of intelligence services: Containing rogue elephants. Routledge.

Bright, D., & Whelan, C. (2020). *Organised Crime and Law enforcement*. https://doi.org/10.4324/9781315522579

Cyber-attacks: Declaration by the High Representative on behalf of the European Union expressing solidarity with Albania and concern following the July malicious cyber activities (2022. September 8). Council of the European Union. https://www.consilium.europa.eu/en/press/press-releases/2022/09/08/cyber-attacks-declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-albania-and-concern-following-the-july-malicious-cyber-activities/

Cottey, A., Edmunds, T., & Forster, A. (2005). Civil–military relations in postcommunist Europe: Assessing the transition. European Security, 14(1), 1–16. https://doi.org/10.1080/09662830500042452

Countering cyber-enabled hybrid interference in the Western Balkans. (2024, December 6). European Union Institute for Security Studies. https://www.iss.europa.eu/publications/analysis/countering-cyber-enabled-hybrid-interference-western-balkans?utm_source=chatgpt.com

Countering cyber-enabled hybrid interference in the Western Balkans. (2024b, December 6). European Union Institute for Security Studies. https://www.iss.europa.eu/publications/analysis/countering-cyber-enabled-hybrid-interference-western-balkans?utm_source=chatgpt.com

Countering hybrid threats. (2026, January 29). NATO. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats?utm_source=chatgpt.com

Countering hybrid threats. (2026b, March 19). EEAS. https://www.eeas.europa.eu/eeas/eu-action-countering-hybrid-threats_en?utm_source=chatgpt.com

DCAF—Geneva Centre for Security Sector Governance. (2017). Intelligence oversight: Ensuring accountable intelligence within a framework of democratic governance. https://www.dcaf.ch/intelligence-oversight-ensuring-accountable-intelligence-within-framework-democratic-governance

Drew S. (2026, March 11). Intelligence Culture and Counterintelligence Effectiveness: Explaining Western European responses to Russian hybrid threats. *FAO Journal of International Affairs*. https://faoajournal.substack.com/p/intelligence-culture-and-counterintelligence

Edmunds, T. (2001). Promoting democratic control of armed forces in Central and Eastern Europe: Lessons learned and future research agendas. Defence Studies, 1, 156–161. https://research-information.bris.ac.uk/en/publications/promoting-democratic-control-of-armed-forces-in-central-and-easte/

Edmunds, T. (2007). Security sector reform in transforming societies: Croatia, Serbia and Montenegro. Manchester University Press. https://gsdrc.org/document-library/security-sector-reform-in-transforming-societies-croatia-serbia-and-montenegro/

European Parliament. (2023). European Parliament recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2023/2500(RSP)). https://eur-lex.europa.eu/eli/C/2024/494/oj/eng

Gentry, J. A. (2022). Cyber intelligence: Strategic warning is possible. *International Journal of Intelligence and CounterIntelligence*, *36*(3), 729–754. https://doi.org/10.1080/08850607.2022.2095544

George, R. (2019). Strategic warning intelligence: history, challenges, and prospects. *Intelligence & National Security*, *35*(2), 310–312. https://doi.org/10.1080/02684527.2019.1603661

Government of Montenegro (2014). Montenegro's Government adopts intelligence and security legislation for national security sector reform. https://www.gov.me/en/article/136228--montenegro-s-cabinet-adopts

Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI). (2026a, March 17). EEAS. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en?utm_source=chatgpt.com

Intelligence and Security Agency of Bosnia and Herzegovina (2026). Establishment. https://www.osa-oba.gov.ba/nase.html

Ioannidis, A. & Kanellopoulos, A. N. (2025) Intelligence Studies Redefined: Designing an Attractive, Structured, and Future-Ready Discipline in Service to the Nation. American Intelligence Journal 42(2).

Kanellopoulos, A.N. & Ioannidis, A. (2023). "The Dimensions of Counterintelligence and Their Role in National Security." *Journal of European and American Intelligence Studies* 6 (2): 85–104.

Kanellopoulos, A.N. (2022). "The Importance of Counterintelligence Culture in State Security." *Global Security and Intelligence* Note 5. https://www.buckingham.ac.uk/wp-content/uploads/2022/07/GSIN_5a.pdf.

Kniep, R., Ewert, L., Reyes, B., Tréguer, F., Cluskey, E. and Aradau, C., (2023). Towards democratic intelligence oversight: Limits, practices, struggles. Kings College London.

https://kclpure.kcl.ac.uk/portal/en/publications/towards-democratic-intelligence-oversight-limits-practices-strugg/

Kosovo Intelligence Agency (2008). The law of Kosovo Intelligence Agency. https://www.aki-rks.org/HTML_ENG/legislation.html

Mobley, B. W., & Wege, C. A. (2021). Counterintelligence Vetting Techniques Compared across Multiple Domains. *International Journal of Intelligence and CounterIntelligence*, *34*(4), 663–693. https://doi.org/10.1080/08850607.2020.1836603

Mobley, B. W., & Wege, C. A. (2021b). Evading Secret Police: Counterintelligence vulnerabilities in authoritarian states. *International Journal of Intelligence and CounterIntelligence*, *36*(1), 179–198. https://doi.org/10.1080/08850607.2021.1937781

Moyers, R. (2025). "Deconstructing and Reconstructing Strategic Counterintelligence Toward a New Model." Studies in Intelligence 69 (2). https://www.cia.gov/resources/csi/static/Article-Moyers-Strategic-Counterintelligence-June-2025-1.pdf.

National Intelligence Service (2026). Our Objective. https://www.nis.gr/en/agency/objective

Parliamentary Assembly of the Council of Europe. (2019). Post-monitoring dialogue with North Macedonia. Report, Document 14964. https://pace.coe.int/en/files/28112

Prunckun, H. (2019). Counterintelligence Theory and Practice. Rowman & Littlefield.

Putter, D., & Bachmann, S. D. (2022). Scoping the future counterintelligence focus. *International Journal of Intelligence and CounterIntelligence*, *36*(2), 358–385. https://doi.org/10.1080/08850607.2022.2091414

Rosenberg, J. (2010). Basic problems in the theory of uneven and combined development. Part II: Unevenness and political multiplicity. *Cambridge Review of International Affairs, 23*(1), 165–189. https://doi.org/10.1080/09557570903524270

Security Information Agency (2026). About Agency. https://www.bia.gov.rs/en/bia/about-agency/

Sithole, T., & Du Toit, J. (2022). A Cyber Counterintelligence Competence framework. *European Conference on Cyber Warfare and Security*, *21*(1), 368–377. https://doi.org/10.34190/eccws.21.1.255

Sofia Military District Prosecutors's Office Filed an Indictment in Court in Case of Espionage Group (2021, November 18). Prosecutor's Office of the Republic of Bulgaria. https://prb.bg/en/news/54670-sofia-military-district-prosecutor%E2%80%99s-office-filed-an-indictment-in-court-in-case

State Agency for National Security of Bulgaria (2026). SIA's Mission is to protect the Security and the Interests of the Republic of Bulgaria. https://www.dar.bg/en

State Intelligence Service of Albania (2026). About Us. https://shish.gov.al/rreth-nesh

Tekorius, A. (2026). Resilience to Threats from Foreign Intelligence Services. In: Schultz, D., Smaliukiene, R., Giedraityte, V. (eds) Democratic Resilience in the Baltics, Vol. 1. Baltic Security and Defense. Springer, Cham. https://doi.org/10.1007/978-3-031-99286-5_5

Walker-Munro, B., & Bachmann, S. D. (2026). Universities as the next counterintelligence battleground in geopolitical contests. *Global Policy*. https://doi.org/10.1111/1758-5899.70167

Declarations

Ethics statement

This article did not involve human participants, personal data, interviews, fieldwork, or classified information.

Funding

The author received no external funding for this work.

Data availability statement

No original dataset was generated or analysed for this article.

Conflict of interest statement

The author declares no conflict of interest.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work, the author used ChatGPT to support structural development, and language refinement. The author reviewed, edited, and approved the final content and takes full responsibility for the submitted manuscript.