International Comparative Jurisprudence 2025 Volume 11 Issue 2
ISSN 2351-6674 (online) DOI: https://doi.org/10.13165/j.icj.2025.11.02.006

INTERNATIONAL EXPERIENCE IN LEGAL SUPPORT OF COUNTERINTELLIGENCE ACTIVITIES AND ITS APPLICATION

Viacheslav Biletskyi[1]
The Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Ukraine
Email: nadpsu@dpsu.gov.ua

Vasyl Korolov [2]
The Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Ukraine
Email: docentpvu@i.ua

Oleksandr Makhlai[3]
The Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Ukraine
Email: naukanadpsu@dpsu.gov.ua

Viktor Tyshchuk[4]
The Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Ukraine
Email: salesmanagement06061976@gmail.com

Vitalii Yeromenko[5]
The Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Ukraine
Email: eremaukraina2014@gmail.com

Received:14 December 2024; accepted: 11 November 2025.
DOI: https://doi.org/10.13165/j.icj.2025.11.02.006

Abstract. This article thoroughly analyses international experiences in the legal support of counterintelligence activities, focusing on the approaches of the UKUSA agreement member countries, European Union states and those in Asia. The main aspects of the legal regulation of special services are discussed, including their organisational structure, mechanisms of democratic control, human rights protection and integration into the international legal system. This article also addresses how counterintelligence agencies respond to modern challenges such as cyber threats and transnational crime. Specific recommendations are offered for adapting leading global practices to Ukrainian realities to enhance the effectiveness of counterintelligence activities, ensure national security and comply with international standards.

Keywords: counterintelligence activities, special services, national security, legal support, international experience.

[1] Candidate of Sciences in Public Administration, head of department at The Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, ORCID ID 0000-0003-0286-097X.
[2] Candidate of Legal Sciences, deputy head of department at The Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, ORCID ID 0000-0002-8342-7557.
[3] Candidate of Psychological Sciences, professor at The Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, ORCID ID 0000-0002-8201-3387.
[4] PhD in Law, associate professor at The Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, ORCID ID0000-0001-5811-5909 (corresponding author).
[5] Senior lecturer at The Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, ORCID ID 0000-0002-9660-8269.

Introduction

Counterintelligence activities are crucial to ensuring national security, especially in the context of escalating threats in a globalised world. Drawing on international experience allows for the development of effective legal mechanisms to address contemporary challenges such as espionage, terrorism and cybercrime. However, since the legal frameworks governing counterintelligence activities vary significantly across countries due to historical, political and geographical factors, it is therefore essential to analyse international experience to craft optimal solutions.

Scholars have devoted considerable attention to studying the legal aspects of counterintelligence. Specifically, researchers have examined the legal frameworks governing the activities of special services in democratic societies and have analysed issues relating to transparency and public oversight. In the context of Ukraine (UA), certain studies focus on adapting the international experience to national needs. At the same time, a comprehensive analysis encompassing the legal frameworks for counterintelligence in leading European Union (EU) countries, the member states of the United Kingdom–United States of America Agreement (UKUSA), and Asia remains insufficient.

This study aims to examine the international experience in the legal regulation of counterintelligence activities and substantiate the possibilities of its adaptation to the reality of the situation in Ukraine. The primary question posed in this article is determining how international experience can contribute to enhancing the effectiveness of national counterintelligence while ensuring adherence to human rights, democratic standards and the rule of law.

The relevance of this study is driven by the need to improve Ukrainian legislation in the context of integration into the European security framework and counteracting internal and external threats. Specifically, the National Security Strategy of Ukraine (Melikhov et al., 2022) emphasises the importance of building a security system based on best international practices. Analysing the legal mechanisms of leading states will aid in formulating recommendations for enhancing the legislative framework of Ukraine (UA).

Thus, the study aims to explore the key approaches to the legal regulation of counterintelligence activities in various countries and to develop proposals for their practical application under conditions in Ukraine. This will strengthen Ukraine's (UA) national security in the face of contemporary challenges.

The theoretical and conceptual framework of the study on the legal regulation of counterintelligence activities is based on integrating several interdisciplinary approaches, including national security theory, legal theory, criminological concepts and doctrines of international law. Given the central research question—how the global experience in the legal regulation of counterintelligence activities can be adapted to Ukrainian conditions—it is crucial to formulate the foundational concepts that define the structure and direction of the analysis.

Counterintelligence activities are considered complex systems comprising search, counterintelligence, regulatory and administrative-legal measures (On et al., 2002). A systematic analysis enables the evaluation of how international standards and practices can be integrated into the national legal and administrative framework. This approach helps identify effective mechanisms for implementing foreign experiences and adapting them to national realities.

One of the key elements of the legal framework for counterintelligence lies in adhering to democratic standards and protecting human rights. The doctrine of the rule of law serves as the foundation for shaping a legal system where counterintelligence measures are conducted in compliance with international law and under the oversight of civilian authorities. This is crucial to adapting Western approaches to legal systems in states who seek to balance security and citizens' rights.

In the context of global threats, counterintelligence must ensure national security without violating citizens' fundamental rights and freedoms. This concept is developed in the works of domestic (Tyshchuk, 2023) and Western scholars, who analyse the optimal balance between the operational effectiveness of special services and adherence to democratic standards. The approach is based on legal oversight and the balance between security and human rights –core principles that can be considered when implementing international experience into Ukrainian practice.

To analyse international experience, it is essential to compare the legal systems of leading countries in counterintelligence. A comparative analysis helps to identify the strengths and weaknesses of different approaches and to determine ways to apply them. This promotes a deeper understanding of the functioning of counterintelligence agencies in various countries and the potential for applying best practices within the national security system.

Counterintelligence services in different countries have their own organisational structure and legal framework, corresponding to national conditions and challenges. However, there is a common understanding that special services form an integral part of the national security system and that their activities must be conducted on the basis of clearly defined legal norms and standards. For Ukraine (UA), it is essential to formulate a legal framework that ensures threats to national security can be effectively counteracted, while also preserving democratic principles and human rights.

The theoretical and conceptual framework of the study therefore allows for delineating the boundaries of the analysis, systematising international experience and identifying the key aspects of its adaptation to the contemporary conditions of Ukraine (UA). This is the foundation for further development of legal recommendations on integrating best international practices in counterintelligence activities.

The study's methodology is based on an interdisciplinary approach that combines several key methods: analysis and generalisation of scientific sources, the comparative-legal method, a systems-structural approach and the modelling method.

The analysis of scholarly works, international agreements and normative-legal acts allowed for key trends in the legal regulation of counterintelligence activities to be identified. The comparative-legal method was used to study the legal systems of leading countries, particularly the legal foundations of the work of counterintelligence agencies, mechanisms of democratic oversight and the protection of human rights.

The systems-structural approach provided a comprehensive understanding of international experience and its potential for integration into national legislation. In light of Ukraine's contemporary security challenges, the modelling method was applied to develop specific recommendations for adapting best practices.

Thus, the chosen methods allowed for a comprehensive examination of the subject, identification of effective approaches and formulation of practical proposals for improving the Ukrainian legal framework.

Artificial intelligence was used exclusively for grammar checking in the preparation of this article.

1. Legal support for counterintelligence activities in countries participating in the "UKUSA" agreement

The legal support for counterintelligence activities in countries participating in the "UKUSA" Agreement – United Kingdom (UK), United States (U.S.), Canada (CA), Australia (AU) and New Zealand (NZ) – has distinct features, based on the principles of cooperation in the fields of intelligence and counterintelligence as outlined by this agreement.

The UK and the U.S. have different types of organisations that protect national security from espionage and terrorist threats. In the UK, the Security Service (MI5, 2024) is relied upon, a purely counterintelligence agency without law enforcement powers, while in the U.S., the Federal Bureau of Investigation (FBI, 2024) serves as a law enforcement agency with counterintelligence functions (Kalkavage and Hulnick, 2014).

The historical development of MI5 has continuously refined counterintelligence work since its inception. Unlike MI5, the history of the FBI reveals an organisation that was initially created for law enforcement purposes and has never been a purely counterintelligence service under the pressure of the U.S. government. This pressure refers to the oversight by the U.S. Department of Justice, to which the FBI belongs, although this is a relatively formal subordination. Such pressure or control from lawyers, which primarily focuses on ensuring legal compliance in procedural actions, can result in breaches of secrecy. In contrast to the American organisation, MI5, which lacks the authority to conduct investigations, is focused on executing counterintelligence activities. This led to more significant efforts to protect the secrecy of its missions, causing MI5 to lose trust in cooperating law enforcement agencies and preventing the full exchange of operational data or joint counterintelligence operations. MI5 has never had law enforcement powers (except for a brief period in the 1990s), whereas the FBI has held such powers since the mid-1930s. Both organisations were similar in the sense that they were both tasked with combating international and domestic terrorism.

The counterintelligence organisations of MI5 and the FBI therefore have respective strengths and weaknesses, which contribute to understanding the key differences between the counterintelligence systems of the U.S. and the UK. A key advantage of MI5 is its focus on conducting counterintelligence activities. In contrast, the FBI's advantage lies in its broader powers, including the ability to investigate crimes against national security.

The modern system of legal regulations that forms the legal basis for the organisation and activities of U.S. counterintelligence can be presented as seen below.

The legal framework for organising and conducting counterintelligence activities in the U.S. is grounded in the U.S. Constitution, which sets out the fundamental principles and structural models of the legal order. It is further elaborated through federal statutes, subordinate regulatory acts, presidential instruments (including executive orders, directives and memoranda), orders and directives issued by agencies subordinate to the President and the strategies, executive documents and directives of the U.S. intelligence and counterintelligence community (Kravchenko, 2018).

It should be noted that in the U.S., the subjects of counterintelligence activities are members of the intelligence community, whose activities are regulated by corresponding normative-legal acts, with the key ones being the public laws "National Security Act" No. 235 (1947) and "The Intelligence Reform and Terrorism Prevention Act" No. 108-458 (2004).

The FBI is the leading agency for detecting, preventing and investigating espionage activities against the U.S. It is responsible for overseeing and integrating the efforts of law enforcement and U.S. intelligence agencies to ensure the utilisation of all available resources to accomplish assigned tasks.

The tasks of FBI counterintelligence work are the protection of the U.S. intelligence community's secrets; the safeguarding of the nation's critical assets-including advanced technologies and sensitive information across the defence, intelligence, economic, financial, healthcare, scientific and technological sectors; the countering of foreign espionage activities; and the prevention of the proliferation of weapons of mass destruction (Federal Bureau of Investigation, 2024).

The National Security Branch (NSB) of the FBI directly carries out counterintelligence activities (Federal Bureau of Investigation, 2024), protecting the U.S. from foreign intelligence and espionage operations through investigations and cooperation with local law enforcement agencies and other members of the U.S. intelligence community.

The NSB consists of units focused on combating terrorism, counterintelligence, intelligence management and weapons of mass destruction.
In addition to the FBI, 17 other well-known U.S. agencies have authority in the sphere of counterintelligence; some of them operate independently, while others form part of the relevant ministries and departments. For example, the U.S. Department of Defense includes at least nine specialised agencies.

Ukrainian scholar Roman Kravchenko (2018) emphasises the fact that according to Order No. 381-20, the U.S. Army has implemented a Counterintelligence Program (Headquarters, Department of the Army, 1993), which outlines that the Army conducts offensive, comprehensive and coordinated counterintelligence activities aimed at detecting, verifying, assessing, countering and preventing foreign intelligence operations, sabotage, subversion, terrorist activities and threats from foreign states, organisations, or individuals against the lives of Army personnel, military equipment and combat capabilities. According to this order, the Deputy Chief of Staff for Intelligence oversees counterintelligence within the Army and implements the Army's Counterintelligence Program. The U.S. Army Commander, along with the Commanders of European, Pacific, Southern and other commands, carries out counterintelligence operations and investigations within their areas of responsibility under the technical oversight of the relevant control departments. Reserve and National Guard commanders conduct relevant counterintelligence activities during mobilisation periods and are responsible for the annual counterintelligence training of Reserve personnel (Kravchenko, 2018). Therefore, counterintelligence is highly integrated into Army structures and subordinated to the military leadership of the U.S. Army.

Justin Harber (2009) argues that for U.S. counterintelligence, understanding the intelligence goals and capabilities of adversaries is crucial and the United States Intelligence Community (USIC) must be prepared to take offensive action, including infiltrating enemy networks and notable service organisations. This tactic of counterintelligence, known as offensive infiltration, serves almost the same function as the work of external intelligence: it uncovers the adversary's capabilities, priorities and operational effectiveness. Perhaps most importantly, it allows the opportunity to disrupt enemy actions through counterintelligence measures such as disinformation. The tactic of offensive counterintelligence involving disinformation measures, as discussed by Harber, is somewhat analogous to the «active measures» employed by the special services of an aggressor state (Tyshchuk, 2024).

Continuing the topic of offensive counterintelligence, it is essential to highlight the words of Frederick Wettering, who points out that the most effective sources for detecting spies in the U.S. are defectors and the spies themselves. Additionally, effective results are achieved through agent-based counterintelligence measures aimed at recruiting personnel from hostile intelligence agencies to identify spies within the U.S. intelligence community (Wettering, 2000).

Although offensive counterintelligence remains one of the best opportunities for the U.S. intelligence community to detect threats to national security, according to Justin Harber, intelligence officials face numerous challenges when infiltrating networks and organisations of hostile intelligence services. For example, U.S. national intelligence agencies are relatively inert targets for adversaries. Their officers often follow similar (standard) tactics resulting from uniform training (Harber, 2009). This points to the need to expand the range of counterintelligence measures and continually alter the algorithms used in their implementation.

All entities involved in intelligence and counterintelligence activities in the U.S. interact within the intelligence community, which is overseen by the Office of the Director of National Intelligence (ODNI), directly reporting to the U.S. president Office of the Director of National Intelligence (n.d.). The structural body of the ODNI is the National Counterintelligence and Security Center (NCSC), which manages national counterintelligence for the U.S. government within the intelligence community.

In light of the above, we can conclude that the FBI is the leading agency for detecting, preventing and investigating intelligence-subversive activities against the U.S. At the same time, the NCSC oversees

national counterintelligence within the U.S. intelligence community for the government (National Counterintelligence and Security Center, 2024).

In addition, it is worth mentioning the counterintelligence powers of one of the U.S. border agencies, the Coast Guard (CG), which is part of the Department of Homeland Security (DHS). The CG has its counterintelligence unit, the Coast Guard Counterintelligence Service (CGCIS). The CGCIS provides counterintelligence support for the Coast Guard's border special operations, protecting personnel, information systems and assets from external enemy intelligence, as well as from the intelligence efforts of terrorist organisations, drug trafficking structures and other organised criminal groups, enemies and spies, as well as from real threats. Furthermore, the CGCIS is responsible for detecting, documenting and investigating non-governmental organisations involved in intelligence-subversive activities and attempting to acquire crucial information about the CG's operations, capabilities, plans and personnel (Coast Guard Counterintelligence Service, 2024).

The UK government has intelligence services with counterintelligence powers within several government departments. These agencies are responsible for gathering and analysing external and internal intelligence information, conducting military intelligence, counteracting espionage and counterintelligence activities. Their intelligence assessments contribute to the conduct of the UK's foreign relations, maintaining national security, military planning and law enforcement activities within the UK. The primary organisations include the Secret Intelligence Service (MI6, 2024), MI5, Government Communications Headquarters (GCHQ, 2024) and Defence Intelligence (DI, 2024).
The Security Service MI5 is the UK's internal intelligence and security agency, part of its intelligence system. MI5 is overseen by the Joint Intelligence Committee (JIC, 2024), supported by the Joint Intelligence Organisation (JIO, 2024), within the Cabinet Office. MI5 is focused on protecting the UK's parliamentary democracy and economic interests and combating terrorism and espionage within the UK (National Intelligence Machinery, 2010).

The legal basis for counterintelligence activities in the UK consists of: The Security Service Act 1989, which entered into force on December 18, 1989 and the Intelligence Services Act 1994, effective from November 2, 1994, together form the foundation of the United Kingdom's counterintelligence legislation. The first section of the Security Service Act 1989 defines the principal function of the leading counterintelligence agency, MI5, as ensuring national security through the prevention and suppression of threats such as espionage, terrorism and sabotage, as well as activities conducted by agents of foreign states or efforts aimed at undermining or overthrowing parliamentary democracy by political, military, or violent means.

The following paragraph of this Act adds the function of "protecting the economic well-being of the UK from threats arising from the actions or intentions of individuals outside the British Isles."

The Security Service Act 1996 amended the previous law, supporting the police and other law enforcement agencies in preventing and investigating serious crimes (Security Service Act, 1996).

Another UK intelligence agency, Defence Intelligence (DI), is also worth mentioning. This organisation is part of the UK's intelligence community and focuses on collecting and analysing military intelligence. Unlike other British intelligence agencies (MI6, GCHQ and MI5), DI is an integral part of the Ministry of Defence rather than a separate entity. The agency employs civilian and military personnel and is funded through the UK's defence budget. Within the Ministry of Defence's Intelligence structure is a counterintelligence directorate whose staff have the appropriate authority to conduct counterintelligence activities (Defence Intelligence, 2024).

Counterintelligence in the UK assesses the country's vulnerability to foreign espionage, monitors sabotage activities and identifies individuals who intend to undermine the established government system. Security measures may be taken based on counterintelligence data. Still, the primary function of counterintelligence is to obtain information on the plans, operations and capabilities of organisations intending to carry out subversive activities. Counterintelligence is conducted in three overlapping

phases: detection, or the recognition of specific factual or obvious evidence of subversive activities; investigation or gathering more evidence; and analysis, which arranges the information in such a way that it can be used. Detection methods include surveillance, publicity (informing the public about the threat of subversive activities) and communication, which allows counterintelligence agencies to cooperate with other public and private security services to maximise the scope of surveillance in detecting subversive activities or legitimate subversive operations (King, 1993).

Matthew Kalkavage and his thesis advisor, Professor Arthur Hulnick, believe that the counterintelligence of the UK is characterised by a focus on recruiting enemy spies and intelligence officers, which, in turn, requires a high level of professionalism from special services personnel in handling double agents. American scholars discuss this element of offensive counterintelligence ("active measures") in the works we mentioned earlier. However, British counterintelligence, due to historical traditions and differences in the powers of the leading national counterintelligence organisations MI5 in the UK and the FBI in the U.S., views the counterintelligence measures of recruitment and working with double agents as a distinct area of counterintelligence activity and strives to excel in this regard (Kalkavage and Hulnick, 2014).

The complexity and ambiguity of working with double agents are highlighted by the words of James Angleton, the former head of counterintelligence at the U.S. Central Intelligence Agency (CIA), who described counterintelligence as a "desert of mirrors." This phrase, borrowed from Thomas Eliot, aptly depicts the endless complexity of possibilities in this mirrored world of distortions. It attempts to understand and outwit the enemy, where it is unbearably difficult to implement the necessary counterintelligence measures. Counterintelligence is a world of truth, lies and deception intertwined in sophisticated ways. As a result of this reality, the leadership of counterintelligence agencies is obliged to strictly adhere to secrecy measures and take additional counterintelligence steps to ensure that double agents provide reliable information. Should they betray them, the damage would therefore be limited to local consequences (Robarge, 2009).

Daniel Lomas and Stephen Ward point out that secrecy has become a core principle for the UK intelligence services due to the focus on working with double agents. Only recently have these intelligence agencies operated in the shadows, not officially recognised by the UK government and lacking the legal foundation at the legislative level. Now, more information about British intelligence is available than ever before and its activities are supported by relevant legislative acts (Lomas & Ward, 2022). This situation is quite similar to our state's, considering the lack of legal and regulatory framework for counterintelligence activities during the Soviet and post-Soviet periods (Table. 1).

Parameters	FBI	MI5
Date of Establishment	July 26, 1908	October 1, 1909
Jurisdiction	National, with limited overseas activity for international investigations	Exclusively national, coordinates international activities through MI6 and GCHQ
Main Functions	Counterintelligence, counterterrorism, organised crime, cyber threats, corruption, intellectual property protection	Counterintelligence, counterterrorism, monitoring extremism, protecting critical infrastructure
Organisational Structure	Over 35,000 employees, including special agents, analysts, technical staff	Approximately 4,500 employees: analysts, operatives, technical specialists
Subordination	U.S. Department of Justice, directly under the control of the FBI Director	The Director reports directly to the UK Prime Minister.
International Cooperation	Joint operations with INTERPOL, EUROPOL, UKUSA partners, bilateral agreements with allies	Close coordination with MI6, GCHQ and other UKUSA partners

Powers	Authorised to make arrests, conduct searches, participate in legal proceedings, initiate criminal cases	Collects intelligence, no authority for arrests or initiating criminal cases
Operational Approach	Operational activities, including covert operations, use of technical means, cooperation with witnesses	Focus on analytical activities, threat prevention and involving individuals.
Funding	Over $10 billion annually (2023)	Approximately £0.6 billion annually (2023)
Management Features	Distributed system with 56 field offices over 350 regional branches, including headquarters in Washington	Centralised management, headquarters in London
Key Tools	Analytical systems, databases, biometric technologies, specialised surveillance programs	Integrated intelligence systems, technical means for communication monitoring
Legislative Basis	Foreign Intelligence Surveillance Act (FISA), sections 18 and 28 of the U.S. Code	Intelligence Services Act 1989, Human Rights Act 1998
Priorities	Counterterrorism, preventing cybercrime, investigating financial fraud	Countering domestic terrorism, protecting national security, analysing extremism threats

Table 1. Comparison of FBI and MI5.

The Canadian Security Intelligence Service (CSIS, 2024) is responsible for counterintelligence functions in Canada. The legislation regulating the activities of CSIS includes the Canadian Security Intelligence Service Act (1984). This act grants the agency the authority to collect and analyse information about national security threats, including terrorism and espionage. Additionally, the Access to Information Act is essential as it provides a certain level of transparency in the operations of intelligence services.

In AU, counterintelligence tasks are carried out by the Australian Security Intelligence Organisation (ASIO, 2024), which operates under the Australian Security Intelligence Organisation Act (1979). According to this law, ASIO can conduct surveillance, wiretapping and other operational measures to combat terrorism, espionage and other national security threats. However, these actions require court approval or the authorisation of specific government agencies to protect citizens' rights.

In New Zealand, counterintelligence activities are carried out by the New Zealand Security Intelligence Service (NZSIC, 2024). Legislative acts, such as the Intelligence and Security Act (2017), define the functions and powers of NZSIC, allowing it to conduct operational measures to identify national security threats, including terrorism and espionage. These measures can only be carried out with the approval of relevant government bodies, ensuring oversight of the intelligence agencies' activities.

All countries signatories to the UKUSA Agreement have legislative provisions ensuring cooperation in intelligence and counterintelligence, as well as restrictions on the use of specific methods such as surveillance and wiretapping. At the same time, each of these countries maintains a balance between national security and citizens' rights, notably through judicial oversight or the need to obtain special authorisations for conducting such operations. An essential role in this process is played by international cooperation within the framework of the UKUSA Agreement, which allows for exchanging information on national security threats and coordinating counterintelligence measures between the countries.

2. The legal framework for counterintelligence activities in European Union countries

Studying the international experience of conducting counterintelligence activities opens up new opportunities for improving the counterintelligence system in the context of its adaptation to the overall European security space requirements. The progressive achievements of countries demonstrating high

professional training for special services personnel and operational units aligned with global standards are exciting to see. These countries have rich historical traditions of special services, which contributes to their leading role in counterintelligence and intelligence activities at both regional and global levels, as well as accumulating significant experience in the professional training of operational personnel to counter new threats to national and state security.

Modern counterintelligence activities in EU countries face enhanced foreign espionage threats, particularly from the aggressor state and the People's Republic of China (PRC). Following the aggressor's invasion of Ukraine, counterintelligence has gained priority status, highlighting the need to improve the legal framework for protecting state interests and EU security. A significant portion of espionage activity is concentrated in Northern Europe, leading to various legal approaches to combat foreign intelligence operations within the EU framework.

Empirical data on espionage in Europe highlights the limited scope of comparative studies in this field, whereas in-depth case studies dominate those that are available. While individual studies help understand the complexity of spies' motivations and the peculiarities of their recruitment, they need to allow for the assessment of the representativeness of specific cases or for forming a comprehensive picture. Available statistical analyses focused on European countries show a predominance of men among convicted spies, with material gain being the dominant motivation and an increasing influence of particular states as initiators of espionage. Most spies are middle-aged individuals, often with experience in military or intelligence fields, although there are also a small number of women. Material incentives are generally accompanied by pressure or threats, although only a few spies receive financial rewards. About 75% of spies are civilians, indicating the growing significance of illicit activities in espionage. The issue of limited access to data complicates comprehensive analysis and existing studies only scratch the surface of the problem, leaving room for hidden cases of espionage (Jonsson, 2023).

Differences between European and American spies manifest in the activity of intelligence-gathering countries. Between 1990 and 2015, the PRC emerged as the primary driver of espionage against the U.S., while the aggressor country remained the leading initiator in Europe, accounting for 37 out of 42 espionage cases. In 2022, despite the rise in Chinese activity, espionage by the aggressor country significantly escalated against the backdrop of the war in UA, with a particular focus on the Baltic states. The situation is further complicated by the uneven geographical distribution of espionage cases and contemporary legislation and political decisions regarding counterintelligence, which influence the number of convictions. In this context, the EU Counterintelligence Course (EUCIC) is a critical tool that provides integrated training for counterintelligence professionals. The course targets professionals with experience in intelligence, investigations and management of agents, aiming to improve skills in line with international and regional standards. Key components of the course include modern counterintelligence methods, security and information analysis, emphasising ethical norms and legal frameworks essential for improving the effectiveness of combating espionage.

A distinctive feature of the course is its inclusion of e-learning modules alongside practical sessions, available as on-site training in Vienna and online. The program covers foundational and advanced aspects of counterintelligence operations, such as mobile and progressive surveillance, working with informants, countering cyber threats, deception and special operations. Candidates also receive comprehensive training in international law and the ethical principles of counterintelligence activities. EUCIC is accredited according to European standards, serving as a benchmark of professional competence in counterintelligence. Thanks to special discounts for distance learning, group bookings and membership, the program remains accessible to various organisational groups, ranging from representatives of government institutions to non-profit organisations and the private sector.

The program's developers believe that the EU Counterintelligence Course provides participants with comprehensive and benchmark training that meets the demands of the modern threat environment and enhances their ability to address the European security community's diverse challenges (Intelligence Academy, 2024).

Counterintelligence functions in the French Republic (FR) are carried out by the General Directorate for Internal Security (GDIS, 2024), established as part of intelligence community reforms through modernisation efforts (Zakharov et al., p. 11-23).

The powers of the GDIS FR exemplify classical approaches to building a counterintelligence system in a democratic country (Ministère de l'Intérieur, 2014), combating foreign interference, including the activities of foreign intelligence services; preventing and stopping acts of terrorism or actions that undermine state security, territorial integrity, or the functioning of French state institutions; preventing and countering actions that expose national classified information or information related to the country's economic, industrial, or scientific potential; monitoring individuals, social movements, groups and organisations engaged in subversive activities or posing a threat; counteracting the unauthorised proliferation of weapons of mass destruction; overseeing the activities of international criminal organisations that may threaten national security; preventing and addressing crimes related to information technologies and communication systems.

At the same time, contrary to international standards, the GDIS is vested with pre-trial investigation functions and can carry out the full range of operational measures typically conducted by structures under the Ministry of Internal Affairs, including the National Police, as stipulated by legislation. The GDIS includes an operational search unit tasked with carrying out arrests, searches and other active operational measures (Zakharov et al., p. 11–23). Thus, the affiliation of this unique service in the FR with the Ministry of Internal Affairs has resulted in law enforcement functions and powers similar to those of the FBI in the U.S.

The reform of France's internal exceptional service attempts to adapt structures established in the 20th century to modern requirements and threats. High-profile terrorist attacks on French soil have become the primary indicator of the success or failure of the GDIS's activities. In most cases, the exceptional service had information about potential terrorists who later became the organisers or perpetrators of terrorist acts in France, yet failed to take practical steps to prevent their plans. As a result, the GDIS is under constant strict control by political forces, particularly the opposition in parliament. This leads to ongoing transformations of the service in its search for the optimal operation model in current conditions (Zakharov et al., p. 11-23).

The exceptional service of the Federal Republic of Germany (FRG) – the Federal Office for the Protection of the Constitution (FOPC, 2024) is part of the Federal Ministry of the Interior. The FOPC is an example of an internal exceptional service with counterintelligence powers. Its primary mission is to protect the state and society from threats that aim to undermine the free democratic order; endanger the existence of the FOPC, the FRG, or any of the federal states; impede the operation of state authorities; act against the FRG's national interests abroad – including through the use of violence; and weaken the foundations of international understanding, particularly the peaceful coexistence of nations.

In addition, the competencies of the FOPC FRG include countering the intelligence and subversive activities of foreign intelligence services, protecting against sabotage and preventing access to confidential information.

The FOPC FRG places particular emphasis on countering far-right, including neo-Nazi parties, far-left, Islamist and other extremist organisations, primarily involving foreign nationals. At the same time, the FOPC FRG is not authorised to conduct pre-trial investigations.

The exceptional service of the Republic of Poland (RP) – the Internal Security Agency (ISA), established in 2002, is responsible not only for counterintelligence tasks, counterterrorism and the protection of state secrets but also for combating the illegal drug trade, organised crime, corruption and economic crimes. Among other duties, the ISA oversees the use of EU funds by Polish state authorities. It monitors the financial activities of government structures, including, for example, the General Directorate for National Roads and Motorways. In contrast to recommended international standards, the ISA is

authorised to conduct criminal investigations, conduct operational search activities, arrest suspects, inspect premises and monitor cargo (Zakharov et al., p. 11-23).

As a result, the activities of the ISA are diverse and resemble the Security Service (SS) of Ukraine (UA) more closely than established European models. In other words, the ISA is not an example of a classical European internal intelligence service created from scratch based on recommendations from countries with developed democracies. Still, it is more akin to a derivative of the special services of post-Soviet countries, which are gradually evolving under the pressure of civil society and through the implementation of democratic civilian oversight. At the same time, alongside the ISA, there operates a separate specialised anti-corruption body in Poland – the Central Anti-Corruption Bureau (CACB, 2024), which is responsible for investigating corruption offenses and has the authority to conduct pre-trial investigations. As a result, there is potential for duplication of functions between the ISA and the CACB, which undoubtedly leads to reduced efficiency in the work of both institutions (Zakharov et al., p. 11-23).

In addition, under the authority of the Minister of National Defence (MND, 2024) of the Republic of Poland (RP), the Military Counterintelligence Service (MCS, 2024) is responsible for protecting against internal threats to national security and defence, as well as ensuring the combat readiness of the Polish Armed Forces.

The Military Counterintelligence Service (MCS) is responsible for tasks such as identifying, preventing and investigating crimes committed by military personnel and employees of the Ministry of National Defence (MND), including crimes against peace, humanity and war crimes that may threaten the security and combat readiness of the Polish Armed Forces; crimes related to the disclosure of classified information; offences involving the trafficking of goods, technologies and services critical to national security; and crimes related to terrorist activities. The MCS coordinates with the military police and other agencies authorised to investigate crimes. It is also tasked with protecting the state by collecting, analysing and processing information related to the defence, security and combat readiness of the Polish Armed Forces. Additionally, the MCS conducts counterintelligence operations in areas such as electronic warfare and cryptographic data protection, participates in planning and monitoring international disarmament agreements, ensures the security of military units and personnel during missions abroad and safeguards scientific research and the production of goods, technologies and services for the Polish Armed Forces. Furthermore, it performs other functions under Polish law and international agreements (Military Counterintelligence Service, 2024).

In summarising the results of this study, we observe a positive experience regarding the counterintelligence systems of the countries discussed, which lies in the integration of counterintelligence into government structures and their subordination to the leadership of the respective authority. At the same time, traditions and former historical models developed in certain countries lead to the preservation of specific functions of special services, which, according to modern international standards, are considered excessive and, in some cases, may threaten human rights. Specifically, this refers to the authority to conduct pre-trial investigations and use coercive measures (including searching private property, arrest, detention and imprisonment). However, the criticism, driven by terrorist activities (September 11, 2001, New York; November 13-14, 2015, Paris; July 14, 2016, Nice), forces special services to gradually change traditional approaches and move towards modern activity formats, which, on the one hand, can ensure the observance of human rights and on the other, increase the effectiveness of special services in fulfilling their tasks. At the same time, the modernisation of special services typically considers international standards in this area, particularly concerning respect for human rights.

Based on the analysis of the development features of the internal special services in the countries discussed, it is considered advisable to ensure the fastest possible transformation of the relevant special services in Ukraine (UA) into organisations focused on countering national security threats within the territory of Ukraine, such as intelligence-subversive activities or their derivative forms, including

terrorism and transnational organised crime, rather than duplicating law enforcement or anti-corruption agencies (Table. 2).

Category	Details	Examples and Sources
General Characteristics	High level of professional training for intelligence agency personnel, adaptation to the European security space	Focus on combating foreign espionage threats, particularly from the PRC and the aggressor country.
Main Challenges	Rise in foreign espionage, increased activity of the aggressor country and the PRC	Central activity regions: Baltic states, Northern Europe
	Uneven geographic distribution of espionage cases	The aggressor responsible for 37 out of 42 espionage cases in Europe (1990–2015)
Counterintelligence Models	EU countries integrate counterintelligence into state structures, considering historical and current demands.	Practical examples: GDIS (FR), FOPC (FRG), ISA (PL)
	Differences in pre-trial investigation approach: GDIS has investigation functions, but FOPC needs such powers.	GDIS performs law enforcement functions similar to the FBI
Counterintelligence Training	EU Counterintelligence Course (EUCIC) – a program for improving the qualifications of counterintelligence specialists according to international standards	Practical sessions in Vienna, online modules, accreditation according to European standards
	Main components: counterintelligence methods, working with informants, countering cyber threats, international law and ethics	The course is available for state authorities and the private sector.
Counterintelligence Services (FR)	General Directorate for Internal Security (GDIS): combating foreign espionage, terrorism, protecting national secrets, countering the spread of WMD	Conducting operational measures, arrests and searches; monitoring terrorist threats
	Under strict parliamentary control, reforms were triggered by terrorist attacks.	Drawbacks: In most cases, the service knew about terrorists but failed to prevent attacks
Counterintelligence Services (Germany)	Federal Office for the Protection of the Constitution (FOPC): protecting democracy, countering sabotage, extremism and subversive intelligence activities	Primary focus: far-right, Islamist organisations, protection from foreign influence
	Lacks pre-trial investigation functions, focuses on prevention and information monitoring	Special attention to neo-Nazi parties and transnational extremist groups
Counterintelligence Services (Poland)	Internal Security Agency (ISA): countering espionage, terrorism, corruption and economic crimes; controlling the use of EU funds	Similar to post-Soviet services, it has pre-trial investigation functions.
	Military Counterintelligence Service (MCS): protecting combat readiness, countering military crimes and cryptographic information control	Interaction with military police, intelligence in the defence sector

Issues and Recommendations	Powers of some services (GDIS, ISA) regarding pre-trial investigations may not meet international standards and pose a risk to human rights.	Recommendations: improving effectiveness through adherence to human rights and international standards
	There is a need for modernisation of services to adapt to modern threats and transnational crime.	Priority: transitioning to modern operational formats with democratic civilian oversight

Table 2. Counterintelligence Activities in EU Countries.

3. Specific legal aspects of counterintelligence activities in Asian countries

In Asian countries, the legal regulation of counterintelligence activities depends on the specifics of state policies and the influence of geopolitical factors. In the People's Republic of China (PRC), the leading agency responsible for counterintelligence operations is the Ministry of State Security (MSS), which has extensive powers to combat threats to national security. The legislation grants it broad authority to carry out various counterintelligence measures, including controlling information flows and monitoring suspicious individuals without a judicial warrant. Under the guise of national security, deep penetration into citizens' data takes place, allowing the MSS to conduct comprehensive analytical operations to identify potential risks (Welch, 2011).

The PRC Anti-Spionage Law (Table 3), which came into effect on July 1, 2023, is a crucial component of the country's legal framework for counterintelligence activities. It significantly expands the powers of relevant agencies, particularly the Ministry of State Security (MSS), providing them with even greater capabilities for controlling information flows and identifying threats to national security. The updated law also strengthens the data collection and protection requirements, significantly affecting foreign companies and individuals working in the PRC.

Category	Details	Examples and Sources
Purpose of the Law	Expanding the scope of protection ("criminalisation") of national security	Strengthening "judicial sovereignty"
Key Changes in the Law	New categories of espionage activity were added, including a collection of commercially significant data.	Article 4(3) covers information previously not considered state secrets (e.g., market data)
	Cyberattacks targeting state organs, infrastructure, or classified information are also considered espionage.	New provisions regarding attacks on critical information infrastructure
Recent Law Enforcement Actions	Raids on consulting firms' offices (Mintz Group, Bain & Co, Capvision) are suspected of gathering information that could threaten national security from the PRC.	The raid at Capvision's office was broadcast live on state media.
	Police seized data, arrested employees and shut down company operations	In the case of Mintz Group, raids led to the closure of the office in Beijing
Scope of the Law	This applies to companies operating in the PRC or processing data related to strategic sectors (e.g., healthcare, technology)	Applies to data with potential value for national security
	Controls the transfer of data abroad, especially in the context of research, mergers and acquisitions (M&A)	The law restricts the transfer of personal data to foreign judicial or law enforcement bodies without permission.

Risks for Foreign Companies	Potential classification of regular commercial activity as espionage (e.g., market research or technology sharing)	Bain & Co. and Capvision were investigated on suspicion of facilitating illegal data collection.
	Increased costs for ensuring compliance with data security legislation	Need for constant monitoring of data sources and compliance with local requirements
Impact on National Security	The law supports the protection of critical information and infrastructure, but it increases tensions in international relations.	Conflicts over restrictions on data transfer between the PRC and international partners
Recommendations for Companies	Strengthen internal protocols: implement data protection policies and avoid unauthorised use of third parties.	Create internal guidelines to prevent data leaks.
	Risk assessment: review supply chains, especially when cooperating with state or suspicious organisations	Bain & Company recommends thorough vetting of third-party agents.
	Investigation protocols: ensure confidentiality of data during international transfer, including anonymity and encryption	Use of anonymised data when working with foreign judicial bodies
Judicial Sovereignty	Prohibition of providing evidence or data stored in the PRC to foreign judicial bodies without government approval	Examples of restrictions in DSL laws (Art. 36), PIPL (Art. 41), ICJAL
Laws Related to CEL	Cybersecurity Law (2017), Data Security Law (2021), Personal Information Protection Law (2021)	Establish standards for data processing and restrict the transfer of confidential information.

Table 3. Changes in China's Anti-Espionage Law and Their Impact (Lamp et al., 2023).

In the Japanese State (JS), counterintelligence activities are carried out by several unique services, with a significant role played by the National Police Agency Security Bureau (NPASB, 2024). The special services in JS operate within stricter legal frameworks, which require judicial oversight of their operations, particularly when intercepting secret communications or conducting searches. To carry out such actions, the agency must obtain a court order to protect citizens' rights and minimise the risk of violations. Additional oversight by the prosecutor's office contributes to more effective compliance with the balance between state interests and individual rights.

In the Republic of India (RI), counterintelligence tasks are carried out by the National Intelligence Bureau (NIB, 2024), one of the oldest intelligence agencies in the world. The primary function of the NIB is to detect threats from foreign intelligence services and counterterrorism. Indian legislation grants NIB broad powers to implement counterintelligence measures, such as phone tapping and surveillance of suspected individuals, making it an effective tool for ensuring national security. However, there is an ongoing public debate regarding the scope of these powers, particularly regarding measures that may infringe on citizens' rights. Despite the existing legal constraints, NIB enjoys government support, allowing it to respond swiftly to national security threats, especially in the face of growing regional risks.

In the Republic of Korea (RK), counterintelligence activities are carried out by the National Intelligence Service (NIS, 2024), which, in addition to protecting against external threats, conducts domestic oversight to prevent espionage activities. Legal regulations limit its actions regarding citizens' personal information, requiring the NIS to obtain court approval for certain types of intelligence activities, such as phone tapping and searches. The legislation of the Republic of Korea regulates the responsibility of special services for abuse of power, which promotes greater transparency and prevents interference in citizens' private lives without proper justification.

In the Republic of Singapore (RS), the role of the counterintelligence agency is performed by the Internal Security Department (ISD, 2024), which has significant powers to combat terrorism and espionage. The ISD has the authority to indefinitely detain suspects without a court warrant if it is deemed necessary in the interests of national security. This legislative provision ensures operational efficiency, but at the same time, raises concerns among international human rights organisations regarding potential violations of human rights.

Thus, the legal aspects of counterintelligence activities in Asian countries demonstrate significant differences in the approaches to regulating intelligence agencies, ranging from democratic constraints in JS and RK to more authoritarian methods in PRC and RS. A common feature across most countries is the attempt to ensure effective counterintelligence in the face of growing international threats. Still, protecting citizens' rights, transparency and oversight of intelligence agencies vary considerably.

4. Proposals for the application of international experience in the legal provision of counterintelligence activities

Integrating the national counterintelligence system into the European and global security space has necessitated the search for and implementation of new approaches to the legal provision of counterintelligence activities based on preserving national achievements and utilising the best practices of global experience. This is emphasised in modern strategic documents of Ukraine, including the National Security Strategy of Ukraine (Melikhov et al., 2021) and Strategies for ensuring state security (2022).

The issue of defining international experience related to implementing counterintelligence measures lies in Ukraine's understanding of national security services, which significantly differs from Western approaches. Specifically, in Western practice, the concept of "intelligence" services generally includes structures that deal with both intelligence (foreign intelligence) and counterintelligence (domestic intelligence) to gather information related to national security threats. Accordingly, the requirements and standards for the activities of intelligence and counterintelligence agencies are based on the same principles of human rights protection and adherence to the rule of law. In other words, in Western practice, there is typically no distinction between "more important" or "more universal" special services. Special services are not categorised by departmental affiliation or functional areas. Each unique service has specific tasks within strict legislative frameworks and under constant democratic civilian oversight. Significantly, this approach not only does not diminish their effectiveness and does not hinder continuous development and improvement, but on the contrary, it leads to continuous updating, modernisation and prevention of abuse (Zakharov et al., p. 11-23).

Alongside this, studying foreign experience in carrying out counterintelligence activities has allowed us to conclude that the aspects set out below could be informative and valuable for domestic legislators.

The experience of the U.S., where the counterintelligence system operates quite successfully, integrated into most key state agencies, primarily those with military and law enforcement orientations, is particularly valuable. The FBI is leading the organisation and coordination of counterintelligence activities in the U.S. At the same time, overall leadership is provided by the interagency body – the NCSC, which is part of the ODNI structure.

The experience of the UK, where counterintelligence is conducted in three overlapping phases, is noteworthy: detection, or the recognition of specific factual or apparent evidence of subversive activities; investigation, or the clarification of additional evidence; analysis, which organises the information in such a way that it can be used within a mechanism for protection of witnesses and victims.

It should be noted that intelligence agencies occupy a special place in the security and defence sector of a democratic state. Despite the varying interpretations and structural peculiarities of special services in each country, there is a common understanding that intelligence agencies are government departments responsible for collecting, processing, analysing and delivering specialised information to relevant state structures that ensure national security. The information provided by intelligence agencies is crucial in

formulating strategic decisions by the country's top leadership and directly influences the functioning of the state, both in domestic and foreign policy (Zakharov et al., p. 11-23).

Conclusions

The comparative assessment of counterintelligence regimes in UKUSA member states, major European jurisdictions and selected Asian systems reveals a set of institutional and legal elements essential for reforming Ukraine's counterintelligence framework. Despite their differing political traditions, effective models consistently combine a clear division of competences, judicial authorisation for intrusive measures and structured oversight mechanisms ensuring transparency and legal restraint.

The contrast between the People's Republic of China and the Republic of India illustrates the boundaries of institutional design. The Chinese model, centred on the Ministry of State Security and not restrained by judicial review, demonstrates the systemic risks of concentrated power and unchecked surveillance. Conversely, India maintains extensive intelligence powers under parliamentary scrutiny, demonstrating that operational effectiveness can coexist with democratic control. For Ukraine, these cases delineate both the practices to be avoided and the benchmarks to be pursued.

Establishing an independent counterintelligence body modelled on the British MI5 – devoid of investigative powers yet operating under strict secrecy – would prevent duplication of functions and strengthen institutional neutrality. Judicial warrants, as required in Japan and the Republic of Korea, should become a prerequisite for any interference with private life, while continuous parliamentary and ombudsman oversight, following the Canadian and Australian examples, would reinforce accountability and public trust.

Further reform should prioritise professional education grounded in legal ethics, cyber counterintelligence and human-rights compliance, alongside the alignment of legislation with GDPR (General Data Protection Regulation) standards on personal data protection. The creation of an independent Human Rights Ombudsman for the security sector would institutionalise preventive monitoring and redress mechanisms.

Collectively, these measures would enable Ukraine to establish a modern, rights-based and resilient counterintelligence architecture consistent with democratic governance and capable of responding effectively to hybrid and technological threats.

References:

Australian Security Intelligence Organisation. (2024). *Australian Security Intelligence Organisation*. https://www.asio.gov.au/
Australian Security Intelligence Organisation Act. (1979). https://www.legislation.gov.au/C2004A02123/latest/versions
Bryja, T. (2024). Winning the Race: The Case for Counterintelligence against Chinese Espionage. *Georgetown Security Studies Review*. https://gssr.georgetown.edu/the-forum/topics/intel-natsec/winning-the-race-the-case-for-counterintelligence-against-chinese-espionage/
Canadian Security Intelligence Service. (2024). *Canadian Security Intelligence Service*. https://www.canada.ca/en/security-intelligence-service.html
Central Anti-Corruption Bureau. (2024). *Central Anti-Corruption Bureau*. https://cba.gov.pl/en
Coast Guard Counterintelligence Service. (2024). *Coast Guard Counterintelligence Service*. https://www.dco.uscg.mil/Our-Organisation/Intelligence-CG-2/
Defence Intelligence. (2024). *Defence Intelligence*. https://www.gov.uk/government/groups/defence-intelligence
Federal Bureau of Investigation. (2024a). *Federal Bureau of Investigation*. https://www.fbi.gov/
Federal Bureau of Investigation. (2024b). *Federal Bureau of Investigation*. https://www.fbi.gov/?came_from=https%3A//www.fbi.gov/about/leadership-and-structure/national-security-branch

Federal Office for the Protection of the Constitution. (2024). *Federal Ministry of the Interior and Community*. https://www.verfassungsschutz.de/EN/home/home_node.html
General Directorate for Internal Security. (2024). *Direction générale de la sécurité intérieure*. https://www.dgsi.interieur.gouv.fr/
Government Communications Headquarters. (2024). *GCHQ*. https://www.gchq.gov.uk/
Harber, J. R. (2009). Unconventional spies: The counterintelligence threat from non-state actors. *International Journal of Intelligence and Counterintelligence, 22*(2), 221–236. https://doi.org/10.1080/08850600802698200
Headquarters, Department of the Army. (1993). *Army regulation 381–20: The Army counterintelligence program*. Washington, DC. https://irp.fas.org/doddir/army/ar381-20.pdf
Intelligence Academy. (2024). *EU Counterintelligence Course (EUCIC)*. https://ieis.eu/covert-operations-training/eu-counterintelligence-course-eucic/
Intelligence and Security Act. (2017). https://www.legislation.govt.nz/act/public/2017/0010/latest/DLM6921247.html
Internal Security Department of Singapore. (2024). *Internal Security Department*. https://www.isd.gov.sg/
Joint Intelligence Committee. (2024). *Joint Intelligence Committee*. https://www.gov.uk/government/groups/joint-intelligence-committee
Joint Intelligence Organisation. (2024). *Joint Intelligence Organisation*. https://www.gov.uk/government/groups/joint-intelligence-organisation
Jonsson, M. (2023). Espionage by Europeans: Treason and counterintelligence in post–Cold War Europe. *Intelligence and National Security, 39*(1), 77–92. https://doi.org/10.1080/02684527.2023.2254020
Kalkavage, M., & Hulnick, A. (2014). *Counterintelligence in the Kingdom and the States: A historical comparison of the FBI and MI5* (pp. 1–87). https://www.bu.edu/pardeeschool/files/2014/08/Sample-Research-Paper-2.pdf
King, D. P. (1993). Counter-intelligence and security. *Police Journal, 66*(3), 306–309. https://doi.org/10.1177/0032258X9306600311
Kravchenko, R. M. (2018). Activities of military counterintelligence in the U.S. Army: Organisational and legal aspects. *Journal Information and Law, 4*(27), 112–120. https://doi.org/10.37750/2616-6798.2018.4(27).273371
Lamp, R., Jun, Y., Wu, W., Zhou, T., & Wang, Z. (2023). China's new counter-espionage law and recent enforcement raise the data security compliance bar. *De Brauw Blackstone Westbroek*. https://www.debrauw.com/articles/chinas-new-counter-espionage-law-and-recent-enforcement-raise-data-security-compliance-bar
Lomas, D. W. B., & Ward, S. (2022). Public perceptions of UK intelligence: Still in the dark? *The RUSI Journal, 167*(2), 10–22. https://doi.org/10.1080/03071847.2022.2090426
Melikhov, O., Yatsyno, O., Shostak, V., Buniak, O., Zatolokin, S., Maslovskyi, S., Sobkovych, S., & Myshalov, D. (2022). *White Book 2021: Defence policy of Ukraine* (pp. 1–122). Ministry of Defence of Ukraine. https://mod.gov.ua/news
Military Counterintelligence Service. (2024a). *Military Counterintelligence Service*. https://www.skw.gov.pl/en/index.html
Military Counterintelligence Service. (2024b). *Military Counterintelligence Service*. https://www.skw.gov.pl/informacje-ogolne.html
Ministère de l'Intérieur. (2014). Décret n° 2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la direction générale de la sécurité intérieure. *Journal officiel électronique authentifié—Décrets, arrêtés, circulaires. Textes généraux*, 0102. https://www.legifrance.gouv.fr/download/pdf?id=E_GVwww232XgTyjxIRx_pLV83fFq1dGGtfc0nz-u5MM=
Minister of National Defence. (2024). *Minister of National Defence*. https://www.gov.pl/web/national-defence/ministry1
National Counterintelligence and Security Center. (2025). *Office of the Director of National Intelligence*. https://www.dni.gov/index.php/ncsc-home
National Intelligence Bureau. (2024). *National Intelligence Bureau*. https://www.mha.gov.in/en/centralpoliceorganisation/intelligence-bureau
National Intelligence Machinery. (2010). *National intelligence machinery* (pp. 1–38). https://www.gov.uk/government/publications/national-intelligence-machinery
National Intelligence Service. (2024). *National Intelligence Service*. https://eng.nis.go.kr/
National Security Act. (1947). https://www.dni.gov/index.php/ic-legal-reference-book/national-security-act-of-1947
National Police Agency Security Bureau. (2024). *National Police Agency Security Bureau*. https://www.npa.go.jp/bureau/security/index.html
New Zealand Security Intelligence Service. (2024). *New Zealand Security Intelligence Service*. https://www.nzsis.govt.nz/
Office of the Director of National Intelligence. (n.d.). *Members of the intelligence community.* https://www.dni.gov/index.php/what-we-do/members-of-the-ic

Verkhovna Rada of Ukraine. (2002). *On counterintelligence activities – Article 1: The concept of counterintelligence activity*. https://zakon.rada.gov.ua/laws/show/374-15?lang=en#Text
Robarge, D. (2009). The James Angleton phenomenon: "Cunning passages, contrived corridors": Wandering in the Angletonian wilderness. *Studies in Intelligence, 53*(4), 1–21. https://www.cia.gov/resources/csi/static/Cunning-Passages-Contrived-Corridors.pdf
Secret Intelligence Service. (2024). *Secret Intelligence Service*. https://www.gov.uk/government/organisations/secret-intelligence-service
Security Service Act. (1989). https://www.legislation.gov.uk/ukpga/1989/5/contents
Security Service Act. (1996). https://www.legislation.gov.uk/ukpga/1996/35
Security Service. (2024). *Security Service (MI5)*. https://www.mi5.gov.uk/
Strategies for ensuring state security. (2022). https://zakon.rada.gov.ua/laws/main/56/2022.?lang=en#Text
The CSIS Act. (1984). https://www.canada.ca/en/security-intelligence-service/corporate/legislation.html
The Intelligence Reform and Terrorism Prevention Act. (2004). *Office of the Director of National Intelligence*. https://www.dni.gov/index.php/ic-legal-reference-book/intelligence-reform-and-terrorism-prevention-act-of-2004
Tyshchuk, V. V. (2023). Features of legal differentiation of the border sphere in Ukraine: Peer-reviewed article. *Italian Review of Legal History, (9)*, 295–329. https://doi.org/10.54103/2464-8914/21918
Tyshchuk, V. V. (2024). Main Criteria for the Classification of Disinformation and Attempts to Criminalisation of Its Spread in Ukraine. *Bratislava Law Review, 8(1)*, 203-224. https://doi.org/10.46282/blr.2024.8.1.372
Welch, J. P. (2011). Chinese counterintelligence: History, tactics and case study. *American Military University*, 1–14. https://www.researchgate.net/publication/257266444_Chinese_Counterintelligence_History_Tactics_and_Case_study
Wettering, F. L. (2000). Counterintelligence: The broken triad. *International Journal of Intelligence and Counterintelligence, 13*(3), 265–300. https://doi.org/10.1080/08850600050140607
Zakharov, Y. Y., Tokariev, H. V., Stupak, I. I., Popov, I. V., Samus, M. M., Semorkina, O. M. (2021). *SBU reform: Challenges and prospects* (pp. 1–172). Ukrainian Institute for the Future. https://archive.khpg.org/en/1608809343