DCAF 25 YEARS

Intelligence Oversight in the Euro-Atlantic Area: Extending to Law Enforcement Functions

Chief Editor: prof. Loch Kingsford Johnson

Andrej Bozhinovski, Pierre Chambart, Teodora Fuior, Henrik Gudmestad Magnusson, Grazvydas Jasutis, Loch Kingsford Johnson, Dragan Lozancic, Mikael Lohse, Grzegorz Małecki, Rebecca Mikova, Nortautas Statkus, Andrius Tekorius, Kristina Vezon, David Watson, Dariia Yarytenko, and Denys Zaskoka

About DCAF

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice, and supports capacity-building of both state and non-state security sector stakeholders. DCAF's Foundation Council members represent over 40 countries and the Canton of Geneva. Active in over 60 countries, DCAF is internationally recognized as one of the world's leading centres of excellence for security sector governance (SSG) and security sector reform (SSR). DCAF is guided by the principles of neutrality, impartiality, local ownership, inclusive participation, and gender equality. For more information visit www.dcaf.ch and follow us on social media.

Acknowledgements

DCAF would like to thank the Federal Department of Defence, Civil Protection and Sport (DDPS) of the Swiss Confederation for its generous support in making this publication possible. DCAF also extends its gratitude to the NATO PA staff and Members of Parliament for their collaboration. The authors greatly appreciate the administrative support provided by Vlasta Kovbasa during the course of the research.

Publisher

DCAF - Geneva Centre for Security Sector Governance
Maison de la Paix
Chemin Eugène-Rigot 2E
1202 Geneva, Switzerland

+41 22 730 94 00

info@dcaf.ch

www.dcaf.ch

Authors: Andrej Bozhinovski, Pierre Chambart, Teodora Fuior, Henrik Gudmestad Magnusson, Grazvydas Jasutis, Loch Kingsford Johnson, Dragan Lozancic, Mikael Lohse, Grzegorz Małecki, Rebecca Mikova, Nortautas Statkus, Andrius Tekorius, Kristina Vezon, David Watson, Dariia Yarytenko, and Denys Zaskoka

Chief editor: Loch Kingsford Johnson

Copy-editor: Aravis Global Advisors

Design and layout: Nadia Joubert

Cover photo: Gorodenkoff, stock.adobe.com

ISBN: 978-92-9222-799-9

Contents

Photo by Gorodenkoff, stock.adobe.com

About the authors

Andrej Bozhinovski is an international legal expert and a doctoral assistant at the Faculty of Law, University of Zagreb, specializing in judicial accountability and criminal justice reform. He has collaborated with DCAF Center for Security Sector Governance, the CEELI Institute Prague, and the U.S. Department of State's INL on regional rule of law initiatives. As founder of the Judicial Media Council, he promotes stronger dialogue between courts and the media. He served as lead author of the CEELI Institute's Guidelines on Judicial Vetting and the Guidelines on Alternatives to Judicial Vetting, developed together with 35 judges from Central and Eastern Europe. His research also focuses on wrongful convictions and the development of Innocence Projects in Croatia and Southeast Europe.

Pierre Chambart served nearly 33 years as a French Army officer in France and overseas. After his retirement in 2019, he co-managed in Baghdad until 2022 the delivery to the Iraqi Intelligence Community's agencies of the European Union-financed program TANSIQ-3 "supporting the development of human rights-compliant counterterrorism strategy, legislation, and coordination measures in Iraq." This program gave him first-hand knowledge of the challenges of Intelligence Sector Reform in post-conflict contexts.

Teodora Fuior is a specialist in democratic governance of the security sector, with over 20 years of experience as a practitioner, researcher, trainer, and project manager. She is a Senior Programme Manager and Security Sector Reform (SSR) Advisor in the Europe Asia Division of DCAF. Teodora leads the Strengthening Security Sector Governance in Moldova Programme and supports other reform-focused processes in countries from the Western Balkans and Eastern Europe. Her areas of expertise include parliamentary oversight, intelligence accountability, the development of legal and institutional frameworks for democratic governance, and human rights implications in the use of intrusive methods for information collection. Besides her extended experience within DCAF Operations and Research Departments, she worked for the Integrated Office of the UN in the Central African Republic (BINUCA), and she served as adviser to the Defence and Security Committee of the Romanian Parliament. Teodora has completed doctoral studies at the National Defence University (Bucharest), with a thesis on democratization and security sector reform in post-conflict states.

Henrik Gudmestad Magnusson has been the director of the Secretariat of the EOS Committee since 2010. Before joining the Secretariat, he had experience working for the Parliamentary Ombud and the National Insurance Court. He has a law degree from the University of Oslo. As the director of the Secretariat, he has led the work of developing the methods and procedures of the EOS Committee, and has first-hand experience of the challenges of being an oversight body.

Grazvydas Jasutis is Principal Programme Manager and Senior Advisor on Security Sector Reform in DCAF's Europe Asia Entity. He leads teams in Geneva and Kyiv working on security sector reform in Eastern Europe, the South Caucasus, and Central Asia. His responsibilities include programs regarding the intelligence sector oversight, both bilateral and in cooperation with Euro-Atlantic institutions. Over the course of his career, he has held senior positions with the EU, NATO, OSCE, and the Ministry of Defence of Lithuania. He is also a prolific author, with over 50 publications to his credit, covering topics ranging from conflict resolution and intelligence sector oversight to post-Soviet security. PhD holder from Vilnius University Institute of International Relations and Political Science.

Loch Kingsford Johnson is Regents and Meigs Professor Emeritus of International Affairs, School of Public and International Affairs (SPIA), University of Georgia. He was a Congressional Fellow in the office of Senator Frank Church (Idaho) in 1969-1970, and subsequently served as his senior aide when Church chaired an investigation of the U.S. intelligence agencies in 1975-76. Professor Johnson was also on the staff of the Senate Committee on Foreign Relations in 1976-77; staff director of the Intelligence Oversight Subcommittee of the House Permanent Select Committee on Intelligence, 1977-79; and senior assistant to the chairman of the Aspin-Brown Presidential Commission on Intelligence, led by Les Aspin in 1995-96. In 2012, the collective universities of the Southeast Conference selected him as their inaugural "SEC Professor of the Year." His most recent books include: The Oxford Handbook of National Security Intelligence (Oxford, 2025); National Security Intelligence (Polity, 2024); The Third Option: Covert Action and American Foreign Policy (Oxford, 2022).

Mikael Lohse is Chief Specialist and Deputy Intelligence Ombudsman at the Office of the Intelligence Ombudsman in Finland. Lohse is an Adjunct Professor, and his research interests include intelligence studies and national security law.

Dragan Lozancic is currently the national security advisor to the President of Croatia. He is a member of Croatia's National Security Council and the National Coordination of Homeland Security, as well as the deputy chairman of the Council for Intelligence Coordination. He is also an international security consultant with over three decades of public service and academic research experience. His prior government postings include being the Director of Croatia's Security-Intelligence Agency, Director of the National Civil Protection Directorate, and Assistant Defense Minister. He was a professor at the College of International and Security Studies (George C. Marshall European Center for Security Studies, Germany) and a defense diplomacy scholar at Cranfield University (UK), where he earned an MS degree in global security studies. He also has a BS from NYIT and an MS, MPhil, and PhD from Columbia University (US).

Grzegorz Małecki is the former head of Poland's Foreign Intelligence Agency (2015-2016). He held the position of the Secretary to the Board for Special Services in the Prime Minister's Office. He was also the First Chancellor at the Polish Embassy in Madrid (Spain). In 2016, he chaired the NATO Civilian Intelligence Committee. After retiring from service, he has been participating in various initiatives related to the reform of special services in Poland

and other countries, and is the author of numerous publications, articles, and press, television, and radio comments and interviews in Polish and foreign media, devoted i.a. to the issues of national security and intelligence services.

Rebecca Mikova is a Project Officer at DCAF, Europe Asia Entity, where she has managed and implemented projects relating to security sector governance in Eastern Europe, the South Caucasus, and Central Asia since 2020. Her work covers defense reform, intelligence reform, and parliamentary oversight. She has led numerous projects relating to mainstreaming human rights and strengthening implementation of international humanitarian law in the armed forces. She holds a Master in International Law degree from the Graduate Institute of International and Development Studies and has published more than 10 studies on various topics relating to good security sector governance and international law.

Nortautas Statkus is the Intelligence Ombudsperson of the Republic of Lithuania and Head of the Intelligence Ombudspersons' Office. He brings over two decades of experience in national security, foreign affairs, and public administration, having held senior leadership and advisory positions at the Ministry of the Interior, the Lithuanian Parliament, the State Security Department, and the Ministry of Foreign Affairs. He also served as an associate professor and research center director at the General Jonas Žemaitis Military Academy of Lithuania. He holds degrees from Vilnius University (BA in History), Central European University (MA in History), the University of London's School of Slavonic and East European Studies (MA), and has pursued Ph.D. studies at Vilnius University's Institute of International Relations and Political Science.

Andrius Tekorius is the chief advisor of the Intelligence Ombudspersons' Office of the Republic of Lithuania. He is an associate professor of practice and teaches intelligence and security courses at the General Jonas Žemaitis Military Academy of Lithuania and Mykolas Romeris University. A. Tekorius is the author of three books and several articles and book chapters on security and intelligence issues. He is the former deputy director of the Lithuanian intelligence service and former national advisor to NATO Allied Command.

Kristina Vezon is a Senior Project Officer at DCAF, where she works on projects related to security sector governance in Eastern Europe, the South Caucasus, and Central Asia. Before joining DCAF, she worked for 6 years at the European Commission on justice and home affairs reforms (including anti-corruption) in Ukraine. She holds an LLM degree from the University of Edinburgh and a Master of Law from Maastricht University and has published multiple studies on topics relating to international law and security sector governance.

David Watson is a former senior UK foreign affairs and intelligence official. He has worked on the reform of Security/ Intelligence Services around the world for the last 12 years. He has worked closely with various governments, DCAF, NATO, and other government agencies during this time.

Dariia Yarytenko is a legal specialist focusing on the regulation of the activities of the Security Service of Ukraine. She obtained her Master's degree in Law from Yaroslav Mudryi National Law University in 2022. She is a participant of the All-Ukrainian School of Criminal Law and Procedure and the Lviv Criminal Justice Forum, an active speaker at academic events and both national and international conferences, and the author of publications in the fields of international law and criminal procedure law.

Denys Zaskoka is a legal expert specialising in the regulation of the activities of the Security Service of Ukraine, a field in which he has worked for the past decade. He graduated in Law from Taras Shevchenko National University of Kyiv in 2001 and has over twenty years of professional experience in the legal sector. In 2025, he was awarded the honorary title of Merited Lawyer of Ukraine.

Chief editor's remarks

Intelligence agencies and the challenges of accountability

Loch K. Johnson

It is a privilege for me to introduce this absorbing set of essays on national security intelligence and the efforts in several nations to ensure that their secret agencies are kept accountable to democratic institutions and principles. This volume gathers together a diverse team of national security experts from several countries among the Western democracies. Their essays provide rare insights into the intelligence organizations in countries that have been leaders in the defence of Western institutions and values, such as France and the United Kingdom, along countries whose secret agencies have been less well studied. These include Croatia, Finland, Lithuania, Norway, Poland, and Ukraine.

Put simply, the core purpose of national security intelligence is to ensure that decision-makers have the best information possible to help illuminate their decision options. Lt. Gen. James R. Clapper Jr., the long-serving U.S. Director on National Intelligence in the United States (2010-2017), has put it well. The objective, he emphasized, is to "eliminate or reduce uncertainty for government decision-makers."[1]

A motto engraved in marble on a wall outside his office in Washington, D.C., read: "Seeking Decision Advantage." The notion is that good intelligence — that is, accurate, comprehensive, timely, and politically neutral information — will lead to more effective choices made by public officials. Decision-makers receive information, of course, from a variety of sources beyond their nation's espionage agencies. As former U.S. Director of Central Intelligence Robert M. Gates (1991-1993) has noted, high officeholders are the recipients of a "river of information" that flows through a nation's capital.[2] This stream of information and policy advice comes from government staffers on defence and security councils; citizen groups; lobbyists; protesters; media reporting; foreign diplomats and heads of state; petitioners and letter-writers, and educators, among others — not to mention family

1 James R. Clapper Jr., 1995. Luncheon Remarks, Association of Former Intelligence Officers, printed in *The Intelligence*, AFIO newsletter, McLean, Va, October, p. 3.

2 Robert M. Gates, 1992. "Guarding Against Politicization," *Studies in Intelligence* 36/5, p.5.

members and friends. Within this flow, however, intelligence gathered from around the world by human assets and surveillance machines guided by intelligence professionals can sometimes provide the most important insights a leader receives (as in the case of the CIA during the Cuban missile crisis of 1962).

In the United States, a simple definition of national security intelligence is the "knowledge and foreknowledge of the world around us — the prelude to Presidential decision and action."[3]

In the United States, a simple definition of national security intelligence is the "knowledge and foreknowledge of the world around us — the prelude to Presidential decision and action."

This statement points to intelligence as a matter understanding events and conditions throughout the world faced by such policymakers, whether presidents, prime ministers, chancellors and their aides; lawmakers; military commanders; diplomats; and trade officials.

Two core truths stand at the heart of this book. The first truth is the notion that secretive intelligence agencies are vital to the domestic and international security of democratic regimes — what U.S. President George H.W. Bush (and former Director of the Central Intelligence Agency or CIA) often referred to as the "first line of defence" for a nation in a hostile global environment. The second truth is that power can be corrupting and secret power especially corrosive to democratic norms, since such power is largely concealed from the public. This is why accountability is so important yet at the same time so difficult, given the darkness in which the secret agencies conduct their affairs.

In this book the reader will find intriguing looks into how secret agencies in a variety of democracies have engaged their executive offices, parliaments, judiciaries, and other organizations — including ombudspersons, human rights commissions, and non-government organizations (NGOs) — as checks on the possible misuse of hidden intelligence powers. This necessity in any genuinely open society is often known as intelligence accountability or oversight.

The imperative of close supervision over secret government organizations is a lesson repeatedly taught by historical experience. In the United States, for instance, investigators in the Congress and the White House discovered in 1975 that the American intelligence agencies had violated the public trust. In violation of its legal charter, the CIA had spied on Vietnam War protesters inside the United States (Operation CHAOS); and the FBI had launched a secret war of espionage and harassment against not only Vietnam War protesters, but civil rights activists as well (Operation COINTELPRO). Further, the National Security Agency (NSA)

3 Central Intelligence Agency, 1991. *Factbook on Intelligence*, Office of Public Affairs, p. 13.

improperly read every international cable sent abroad or received by an American citizen (Operation MINERET).

Military intelligence units also spied on student demonstrators within the United States. Then, more recently in 2013, a leak to the *Washington Post* revealed that — once again — the NSA was misusing its surveillance powers to spy on American citizens by massively collecting information on the patterns of their telephone conversations.[4] Further, at presidential insistence during the George W. Bush presidency, the CIA had resorted secretly to the use of torture methods against suspected 9/11 terrorists, despite the strong moral opprobrium these methods carry and without the knowledge of the congressional oversight panels.

Once these activities were disclosed by congressional investigators over the years, new legislation tightened control over America's secret agencies and banned torture. All the good work these agencies had carried out against the Soviet Union during the Cold War was stained by these excesses and demanded tighter control by legislative, judicial, and executive intelligence overseers. The era of new and more serious intelligence accountability in the United States began in earnest during 1975 with the Church Committee inquiries and continues today.[5]

Throughout the universe of democratic nations, large and small (which collectively remain outnumbered by the world's authoritarian regimes), an ongoing search continues for the proper balance between the close supervision of intelligence under the law, on the one hand, and sufficient executive discretion to permit the effective conduct of vital intelligence missions against foreign autocrats and domestic insurrectionists, on the other hand. The essays in this book contribute significantly to this search, with a sensitivity to both of these important objectives.

It is a pleasure to welcome you to these pages.

4 Loch K. Johnson, 2015. *A Season of Inquiry Revisited: The Church Committee Confronts America's Spy Agencies*. Lawrence: University Press of Kansas.

5 Loch K. Johnson, 2018. *Spy Watching*. New York: Oxford University Press.

Photo by hanmaomin, stock.adobe.com

Executive summary

DCAF and the NATO Parliamentary Assembly have collaborated to publish a report that focuses on the democratic governance and oversight of intelligence agencies, mainly those with law enforcement powers. It emphasizes that the supervision of intelligence in a democracy relies not only on suitable institutional designs but also on legitimacy, transparency, and multi-layered accountability. The report gives a detailed analytical framework and also throws light on the comparative states in relation to the separation of intelligence and law enforcement powers in the Euro-Atlantic area, as well as on the mechanisms that ensure accountability and respect for the rule of law. The first section of the paper, *Conceptual Foundations*, explains and follows the development of intelligence services with law enforcement capabilities, investigating to what extent their blurred boundaries with law enforcement institutions have influenced democratic control. The study delves into the historical and legal contexts of these overlaps. Therefore, this part lays down the conceptual and normative foundation for comprehending the intricate relationship of intelligence operations, state security, and individuals' rights. The second part, *Oversight and Accountability Mechanisms*, examines the institutional structure that enables parliaments, governments, courts, and civil society to oversee the activities of the intelligence sector.

The third part, *Regional Case Studies*, examines practical experiences from France, Lithuania, Norway, UK, Poland, Finland, Croatia, and Ukraine. These examples illustrate different institutional arrangements ranging from parliamentary commissions and inspector-general offices to judicial review and ombudsperson mechanisms and how they contribute to accountability and public trust. The case studies reveal that while legal frameworks differ, shared principles of transparency, professionalism, and respect for rights underpin successful oversight models.

The study concludes that effective oversight depends more on the presence of political will, expertise, and persistence than it does on resources. Using comparisons, it demonstrates the importance of cooperation between oversight actors, the sharing of information, and the establishment of joint inquiry mechanisms across parliaments.

Photo by Framestock, adobe.stock.com

Part I:
Conceptual foundations

1.1. Defining intelligence services with law enforcement mandates: Evolution, boundaries, and overlaps

Dragan Lozancic

1.1.1. Introduction

We should first, argued a Western analyst, Larry Watts, identify and agree on what constitutes intelligence 'best practice', even if we do not yet meet all the standards ourselves.[6] This was a reference to reforms in post-authoritarian, emerging democracies aspiring for Euro-Atlantic membership. But as much as it was a call for establishing common standards, it was also a candid admission that some democracies may not be practicing what is preached on their behalf. And nowhere would this be more evident than in urging European Union (EU) aspirant countries to separate law enforcement powers from their intelligence services.[7] While some aspirant countries complied, others were more reluctant. Nevertheless, recent EU enlargement reports have stressed the importance of independent oversight and called out candidates whose intelligence services' powers overlapped with those of the police or law enforcement authorities.

Ukraine is an example. The mandate of Ukraine's security service 'should focus on its national security tasks,' it was claimed in a recent report, further suggesting its ''pre-trial investigation functions should be transferred to… dedicated law enforcement agencies''.[8] This was nothing new to Ukraine's authorities. For over a decade, Ukraine's Western partners, both governmental and non-governmental, as well as its own domestic human rights groups, have been advocating for the scaling down of the security service's outsized powers, particularly its law enforcement role. The service had been marred by allegations of corruption and politically motivated investigations.[9] Despite its current existential struggle against Russian aggression, questions over whether its security service should retain a law enforcement mandate will continue to be central in Ukraine's intelligence reforms.

6 Watts, L.L., 2004. 'Intelligence Reform in Europe's Emerging Democracies'. *Studies in Intelligence* 48/1, 11–25 at 25.

7 The term 'intelligence service' will be used generically, including sometimes inferring to 'security services', unless specified as strictly 'foreign' (external), domestic (internal), 'military' or otherwise.

8 European Commission, 2024. *Georgia 2024 Report: 2024 Communication on EU Enlargement Policy*, *SWD(2024) 697 final*. Brussels, 30 October, 41.

9 Kramer, A.E., 2024. 'Dysfunction Sidelines Ukraine's Parliament as Governing Force', *The New York Times*, 16 July. Available at: https://www.nytimes.com/2024/07/16/world/europe/ukraine-parliament.html [Accessed 12 January 2025]; Fluri, P. and Polyakov, L., 2021. 'Intelligence and Security Services Reform and Oversight in Ukraine – An Interim Report'. *Connections: The Quarterly Journal* 20/1, 51–59 at 51.

Domestic intelligence services have been objects of numerous international studies (e.g. DCAF, Venice Commission, and Council of Europe). Most scholars have had democracy's best interests in mind, uncompromisingly promoting security, good governance, and the rule of law. These studies shared similar concerns and suggested that a set of common standards be adopted. But separating law enforcement powers from intelligence services would remain an open and elusive issue.[10] Even among European countries there was no meaningful consensus. However, the Parliamentary Assembly of the Council of Europe would be more forthcoming. It decisively recommended that intelligence and law enforcement functions be strictly separated. The main worry was the potential abuse of power when the two functions were to be found within the same institution. Most internal security services across the Euro-Atlantic area do not have law enforcement mandates. The same is true of Australia, Canada, Japan, New Zealand, South Korea, Switzerland and many others. But a handful of democracies maintain security services with law enforcement mandates. Unanimity in favour of one model over the other may be out of reach for now. But there is a staunch consensus on assuring executive control, safeguards against abuse, independent oversight, and accountability, standards that become even more important with increased power and authority. Given that many cases of abuse of power are exposed by investigative reporting, having a strong independent press is essential.[11]

1.1.2. Evolution of domestic/internal intelligence

Intelligence communities in liberal democracies come in different shapes, forms, and sizes. The evolution of each country's approach is as unique as its own special set of historical, political, and cultural circumstances. But some general, widely practiced characteristics have emerged. Countries typically have separate civilian and military intelligence organisations. Most also have separate foreign and domestic intelligence services. Exceptions with a single civilian service responsible for foreign and domestic intelligence include Croatia, Cyprus, Greece, Lithuania, Luxembourg, Malta, the Netherlands, Slovakia, Slovenia, Spain, and Switzerland, as well as Albania, Bosnia and Herzegovina, Kosovo, Montenegro, Serbia, and Moldova. Of these, only Serbia's BIA has a law enforcement mandate. After the 2015 Paris terrorist attacks, a French parliamentary commission set up to investigate the failures that led to the attacks recommended that the country's multiple intelligence agencies be merged into a single agency.[12]

10 Watts, 2004. 'Intelligence Reform', 24.

11 Johnson, L.K., 2017. *Spy Watching: Intelligence Accountability in the United States*. Oxford: Oxford University Press.

12 Calamur, K., 2016. 'Overhauling French Intelligence Agencies'. *The Atlantic*, 5 July.

Table 1. Security services of European and EU aspirant countries

European Internal Security Services		
Do not have law enforcement powers		Have police/law enforcement powers
▪ Belgium ▪ Bulgaria ▪ Croatia ▪ Cyprus ▪ Czech R. ▪ Germany ▪ Greece ▪ Hungary ▪ Italy	▪ Lithuania ▪ Luxemburg ▪ Malta ▪ Netherlands ▪ Portugal ▪ Romania ▪ Slovakia ▪ Slovenia ▪ Spain	▪ Austria ▪ Denmark ▪ Estonia ▪ Finland ▪ France ▪ Ireland ▪ Latvia ▪ Poland ▪ Sweden
Internal Security Services (EU aspirants)		
Do not have law enforcement powers		Have police/law enforcement powers
▪ Albania ▪ Bosnia & Herzegovina ▪ Kosovo ▪ Montenegro	▪ N. Macedonia ▪ Moldova ▪ Türkiye	▪ Georgia ▪ Serbia ▪ Ukraine

Today's intelligence organisations mandated with police or law enforcement powers are, by and large, identified as domestic intelligence or security services. Who created the first modern (domestic) intelligence service? Was it the British, the French or was it someone else? Britain's MI5 began operations as the Secret Service Bureau in October 1909.[13] But it operated in the shadows for most of the subsequent century, its existence was only publicly acknowledged with the Security Service Act of 1989, establishing a formal statutory basis for MI5 for the first time. The Act came about, in part, because of European court rulings proscribing interference with human rights without some basis in domestic law as unacceptable.[14] The French may have an earlier claim. French intelligence emerged as an internal police function and became a permanent state feature in the late nineteenth century.[15] Not to be outdone, Serbia also has a claim to having the oldest domestic intelligence service: its former director says it came into being

13 Andrew, C., 2009. *The Defence of the Realm: The Authorized History of MI5*. London: Penguin Group, 3.

14 Andrew, 2009. *The Defence*, 759.

15 Bauer, D., 2021. 'Marianne Is Watching: Intelligence, Counterintelligence, and the Origins of the French Surveillance State.' Lincoln: University of Nebraska Press.

in 1899.[16] Yet, the conceptual origins of all three, or of any other pretender for that matter, are probably more deeply rooted.

'Within this very body are enemies; within this most sacred and honourable council' Marcus Tullius Cicero warned the Roman Senate in 63 BC, 'there are those who are thinking about the destruction of all of us'.[17] The idea of an enemy or a threat 'from within' is one of the oldest fears of human civilizations. It is also one of the most enduring, as the US Vice President J.D. Vance reminded his European allies in February 2025 at the Munich Security Conference: 'what I worry about (most) is the threat from within.' The threat from within is as challenging to our modern nation states, as it was for the city-states, kingdoms, and empires of the past. None were immune regardless of their system of government. China's communist leaders have purposely distributed surveillance tasks to different security units for fear of creating a too 'powerful secret police' or other potential rivals to its own power.[18]

In fact, totalitarian states, dictatorships, authoritarian governments, and other non-democratic regimes have been particularly attentive. Authoritarian rulers, as fearful of the populations they governed as of rivals within their own regimes, found it difficult to survive without political or secret police forces.[19] Eliminating threats from dissidents and political opponents was critical. 'Authoritarian regimes can fail at everything, and they often do,' according to Stephen Kotkin, 'but they survive as long as they succeed at one thing—the suppression of political alternatives'.[20] In Eastern Europe, there are painful memories of the security services of an earlier era, services that indulged in blackmail, torture, and assassination.[21]

Counter-intelligence (CI) emerged as a domestic complement to a nation's foreign intelligence efforts. It was supposed to deal with espionage and sabotage stemming from foreign actors or their local proxies and agents, especially in wartime. During the Cold War, domestic intelligence was almost exclusively concerned with rooting out foreign spies and traitors. In the US, a pervasive fear of communist infiltration led the FBI to focus its efforts on Soviet operatives and homegrown sympathizers. It would be accused of unwarranted excesses in targeting individuals and organisations involved in legitimate political activities.[22] Its notorious COINTELPRO operations (1956-1971) aimed at civil rights and

16 BIA – Security-Intelligence Service, 2019. 'The speech of the Director of the Security Information Agency, Mr. Bratislav Gašić, BIA Anniversary 2019'. Republic of Serbia. Available at: https://www.bia.gov.rs/en/media/public-statements/the-speech-of-the-director-of-the-security-information-agency-mr-0/ [Accessed 25 January 2025].

17 Cicero, 1976. *In Catilinam 1–4. Pro Murena. Pro Sulla. Pro Flacco*. Cambridge, MA: Harvard University Press.

18 Pei, M., 2024. 'Why China Can't Export Its Model of Surveillance'. *Foreign Affairs*, 6 February.

19 Mehrl, M. and Choulis, I., 2024. 'Secret Police Organizations and State Repression'. *Journal of Conflict Resolution* 68/5, 993–1016.

20 Remnick, D., 2025. 'Can Ukraine — and America — Survive Donald Trump?'. *The New Yorker* (interview with Stephen Kotkin), 9 March.

21 Smith, C.S., 2006. 'Eastern Europe Struggles to Purge Security Services'. *The New York Times*, 12 December.

22 Sullivan, J.P. and Lester, G., 2022. 'Revisiting Domestic Intelligence'. *Journal of Strategic Security* 15/1, 75–105.

anti-war movements undermined US democracy.[23] It had looked to discredit and neutralize those it considered subversive elements within the country, ever ready to use secret and unlawful means to criminalize various forms of political struggle. The FBI's long-serving director J. Edgar Hoover had mastered manipulating the Agency's counter-intelligence and law enforcement mandates, often employing intimidation and blackmail.[24] Europe too was a hotbed of East-West espionage. But it also had its share of controversy. In the UK, revelations emerged of the widespread surveillance and telephone wiretapping of political activists and trade unions.[25] Counterintelligence efforts have traditionally struggled to differentiate between real and imaginary threats. Western democracies find little comfort in the thought that such antics paled in comparison to authoritarian or totalitarian systems. As a result, to protect rights, the rule of law, and democracy itself systemic norms emerged including clear intelligence legislation, independent oversight, safeguards, and accountability.

The counterintelligence mission expanded when the Berlin Wall came down. Former enemies would now be partners. Counterintelligence took on a broader set of tasks, including dealing with terrorism, violent extremism, illicit trafficking and transnational organised crime (e.g. drug cartels), and cyber threats. Terrorist attacks would be particularly consequential. These new challenges blurred the line between foreign and domestic threats. But also between national security and law enforcement. Counterespionage would take a back seat to counterterrorism, which required much wider interagency coordination and cooperation. Intelligence would emerge as a fundamental security tool on the home front. Moreover, counterintelligence had now become synonymous with domestic intelligence.[26]

The secret police and counterintelligence dimensions have thus come to shape contemporary domestic intelligence services. For post-authoritarian democracies, an important challenge was deciding what to do with the inherited police powers or law enforcement mandates of their intelligence services. Among liberal democracies, different models co-exist without too many hang-ups. For example, Germany's domestic intelligence service BfV (*Bundesamt für Verfassungsschutz*) does not have any law enforcement powers. Due to its traumatic experience with the *Gestapo*, post-war Germany decided to strictly separate intelligence and law enforcement. The extent of this separation is so far reaching that it encompasses functional, organisational, and informational spheres.[27] Ensuring a further dispersal of power, domestic intelligence is also regionally decentralized to reflect Germany's sixteen federal states (*Länder*). On the other hand, Sweden's security service

23 Johnson, L.K., 2017. *Spy Watching: Intelligence Accountability in the United States*. Oxford: Oxford University Press, xi.

24 Gage, B., 2022. *G-Man: J. Edgar Hoover and the Making of the American Century*. New York: Viking, vi.

25 Leigh, I. and Lustgarten, L., 1989, The Security Service Act 1989'. *The Modern Law Review*, 52/6, 801.

26 Sullivan and Lester, 2022. 'Revisiting Domestic Intelligence', 76; DCAF, 2020. 'Counterintelligence and Law Enforcement Functions in the Intelligence Sector'. Thematic Brief. Geneva: DCAF.

27 Haldenwang, T., 2022. 'Chapter VIII: Germany'. In: P. Burczaniuk, ed. *Legal Aspects of the European Intelligence Services' Activities*. Warsaw: Internal Security Agency (Poland).

SÄPO (*Säkerhetspolisen*) has law enforcement powers and is considered both an intelligence and police service. It can investigate crimes, collect evidence, and make arrests. While there is a clear demarcation of responsibilities between the police and SÄPO, jurisdictional overlaps occur in certain circumstances.[28] In that sense, Germany and Sweden have somewhat differing perspectives on domestic intelligence. Nevertheless, both countries have high standards of protection against abuse. Among the world's liberal democracies, most have chosen to separate law enforcement and intelligence.

1.1.3. Defining Domestic Intelligence

There is no widely accepted, single definition of domestic intelligence. Intelligence as a state function serves to safeguard national security. Few will argue with that. Unlike its foreign component, the intrusiveness of domestic intelligence is potentially much more likely to resonate within the country. Individual citizens' rights and freedoms are more likely to be directly affected. Likewise, domestic intelligence efforts are more likely to be drawn into contentious partisan politics, certainly more so than foreign efforts. Germany's domestic intelligence service caused a storm of controversy when it publicly labelled Germany's main opposition party *Alternative für Deutschland* (AfD), as a 'confirmed right-wing extremist' entity.[29] It must be remembered that AfD received over twenty percent of the vote in the last parliamentary election. Controversy was also stirred when a high court in Romania annulled the first round of presidential elections on the basis of information provided by its own security service. A free and fair election process is one of the most sacred rituals in any democracy. Unhappy with the outcome, many Romanian voters were ambivalent about the court's intervention and the role of intelligence.[30] Both cases illustrate the risks and consequences of domestic intelligence efforts.

According to Posner:

> *'domestic national-security intelligence is concerned with the 'threat of major, politically motivated violence, or equally grievous harm to security or the economy, inflicted within the nation's territorial limits by international terrorists, homegrown terrorists, or spies or saboteurs employed or financed by foreign nations'.*[31]

28 Cameron, I., 2023. *National Security Surveillance in Sweden. Safe and Free: National Security Surveillance and the Rule of Law Across Democratic States*. Available at: https://safeandfree.io/wp-content/uploads/2023/11/Sweden_Surveillance_FINAL.pdf [Accessed 8 May 2025].

29 Janjevic, D., 2025. 'German AfD party labeled "extremist" by intelligence agency'. *Deutsche Welle*, 2 May.

30 Higgins, A., 2025. 'Romanian Nationalist Wins First Round of Presidential Voting'. *The New York Times*, 4 May.

31 Posner, R.A., 2005. 'Remaking Domestic Intelligence'. American Enterprise Institute for Public Policy Research, AEI Working Paper 111, 1-2. Available at: https://www.aei.org/wp-content/uploads/2011/10/20050621_DomesticIntelligence3.pdf?x85095 [Accessed 6 March 2025].

A RAND study describes domestic intelligence as government efforts to gather, assess, and act on information about individuals or organisations within a country or its citizens abroad.[32] These efforts are not necessarily related to the investigation of a known past criminal act or specific planned criminal activity.[33] Most others steer clear of a clear-cut definition.[34] On the other hand, the UK's Security Service Act 1989 provides a simple, yet well-articulated account of what a domestic security service is all about. According to Section 1 of the said Act, its function is to protect national security, from espionage, terrorism and sabotage, as well as from the acts by foreign agents and others that aim to overthrow or undermine democracy by political, industrial or violent means; it also mentions contributing to safeguarding the country's economic well-being and providing support to law enforcement (especially in relation to serious crimes). It does not include law enforcement responsibilities or police powers. Similar functional descriptions, perhaps in greater or lesser detail, are to be found in many other Western democracies.

Table 2. Internal Security Services (other Western democracies)

Internal Security Services	
Do not have law enforcement powers	Have police/law enforcement powers
▪ Canada ▪ U.K. ▪ Switzerland ▪ Iceland ▪ Australia ▪ New Zealand ▪ South Korea ▪ Japan	▪ U.S. ▪ Norway

The United States (US) intelligence community is in a league of its own. It is composed of eighteen separate organisations, including independent agencies and departmental organisational units. The *Washington Post* described it as becoming 'so large, so unwieldy and so secretive that no one knows how much money it costs, how many people it employs, how many programs exist within it or exactly how many agencies do the same work'.[35] The US does not have a single institution responsible for domestic intelligence and instead relies on multiple organisations that are loosely related and that often compete.[36] Also, the US has tended to treat domestic intelligence, other than internal security threats and

32 Jackson, B.A., ed., 2009. The Challenge of Domestic Intelligence in a Free Society. Santa Monica: RAND Corporation, 3-4.

33 Jackson, 2009, *Challenge*.

34 Sullivan, and Lester, 2022. 'Revisiting Domestic Intelligence', 76-8; Burch, J., 2007. 'A Domestic Intelligence Agency for the United States? A Comparative Analysis of Domestic Intelligence Agencies and Their Implications for Homeland Security'. *Homeland Security Affairs* III/2, June. Available at: https://casi.sas.upenn.edu/sites/default/files/iit/Burch%2C%20Domestic%20Intelligence%20Agencies%20-%20Related%20Resources.pdf [Accessed 6 March 2025].

35 Priest, D. and Arkin, W.M., 2010. 'A hidden world, growing beyond control'. *The Washington Post*, 19 July, A1, A6–A9. Available at: https://www.pulitzer.org/cms/sites/default/files/content/washpost_tsa_item1.pdf [Accessed 28 April 2025].

36 Sullivan and Lester, 2022. 'Revisiting Domestic Intelligence', 96.

especially before the September 11 terrorist attacks, as a law enforcement issue.[37] The FBI is perhaps the most important example. While the FBI shares some of the hallmarks of its European security service counterparts, especially in its counter-intelligence mission, it is primarily a federal law enforcement agency with a criminal investigation/conviction culture overshadowing its national security role.[38] The creation of a domestic intelligence agency, separate from the FBI and strictly dedicated to national security, has been a decades old debate in US government and academic circles.[39]

While common experiences or shared understandings persist, each country's decision to establish a domestic intelligence service with or without a law enforcement mandate has its own background. The Canadian Security Intelligence Service (CSIS) emerged in 1984 after an independent investigation (McDonald Commission) found its predecessor, the RCMP Security Service, had abused its powers and was involved in numerous illegal activities. One of the main recommendations was to set up a separate civilian intelligence agency with no law enforcement functions. Many East European countries have also opted to separate out the two functions.

Following a mass wiretapping scandal in 2015, North Macedonia decided to transform its counterintelligence and police-based security service, UBK into the National Security Service (ANB). This would be a domestic intelligence service with no police powers or law enforcement responsibilities. Moldova shed its Soviet roots when it amended legislation in 2005 to strip the Security and Intelligence Service of its law enforcement mandate. To further transform intelligence into a modern, Western-type service, Moldova's government has been looking to make clearer distinctions between intelligence activities and criminal investigations.[40] While Georgia's State Security Service was separated from the Interior Ministry in 2015, it still maintains an extensive law enforcement mandate with criminal investigations and powers of arrests. Georgia has been urged to strip its security service of anti-corruption investigative powers.[41] Pointing to Georgia's weak oversight capabilities, international observers and non-governmental organisations are calling for further intelligence reforms.

---

37 Lowenthal, M.M., 2020. *Intelligence: From Secrets to Policy*, 8th ed. London: SAGE Publications Ltd, 7.

38 Posner, R.A., 2006. 'The Reorganized US Intelligence System, after One Year'. American Enterprise Institute for Public Policy Research, Special Edition, 5.

39 Sullivan and Lester, 2022. 'Revisiting Domestic Intelligence'; Posner, R.A., 2011. *Remaking Domestic Intelligence*. Stanford: Hoover Institution Press; Schaefer, A.G., et al., 2009. *The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency*. Santa Monica: RAND Corporation. Available at: http://www.jstor.org/stable/10.7249/mg804dhs [Accessed 14 April 2025]; Burch, J., 2007. 'A Domestic Intelligence Agency; Posner, 2006. 'The Reorganized US Intelligence System'; Masse, T., 2003. 'Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States'. Congressional Research Service, RL31920. Available at: https://www.everycrsreport.com/files/20030519_RL31920_f37f2e430c19429d72e67e24d7ec8524e4554bd3.pdf [Accessed 14 April 2025].

40 Venice Commission, 2023. *Republic of Moldova: Follow-Up Opinion to the Opinion on the Draft Law on the Intelligence and Security Service, as Well as on the Draft Law on Counterintelligence and Intelligence Activity, CDL-AD(2023)008*. Strasbourg, 9 October.

41 European Commission, 2024. Ukraine 2024 Report: 2024 Communication on EU Enlargement Policy, SWD(2024) 699 final. Brussels. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024SC0699 [Accessed 6 March 2025], 38.

Denmark, Finland, Norway and Sweden, on the other hand, maintain a Nordic tradition of closely linking intelligence with police organisations. Their services have law enforcement mandates and police powers. These same Nordic countries consistently rank at the very top of several independent index measurements of the world's most democratic countries (civil liberties, political participation, and the rule of law). However, each is unique. For example, SUPO, Finland's interior-ministry-based intelligence agency likes to emphasize that its investigative role is mainly focused on 'state security-related' crimes and that it relies on the police to make actual arrests. It is clearly different from Sweden's security service SÄPO, which is a stand-alone organisation that investigates and regularly makes its own arrests. See Vrist Rønn *et al*. for additional insights into a Scandinavian approach to integrating police-intelligence functions and for an account of how these Nordic countries have managed to uphold a high level of public trust.[42]

The countries that have emerged from the former Soviet Union have all, except Lithuania and Moldova, retained intelligent services with law enforcement powers. Nevertheless, Estonia, Latvia, Lithuania, Georgia, Moldova and Ukraine have transformed or are transforming their security services to resemble Western models of governance and oversight. The security services of the rest—Armenia, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, Turkmenistan and Uzbekistan—are to a greater or lesser extent KGB successors. Intelligence has long been considered a fundamental tool for combating criminal threats, according to a group of Russian analysts, especially in dealing with 'crime(s) that (are) not covered by criminal legislation' and 'criminal actions that have not taken the form of crimes'.[43] The potential for abuse and the risk of arbitrary enforcement efforts cannot be underestimated. The mandate of Russia's Federal Security Service (FSB) includes law enforcement functions, although its role and influence go well beyond its constitutionally granted powers.[44] As a security service, the FSB plays a central role in dealing with the regime's enemies at home and abroad.[45] According to Articles 8, 10, and 12 of the Federal Law on the Federal Security Service of the Russian Federation, the FSB's law enforcement tasks cover a wide range of criminal activities. The FSB also has border security responsibilities, and according to Article 15 of the Federal Law mentioned above, its officers are authorized to use military equipment and combat tactics. It is hard to find a security service among Western democracies with comparable *de jure* or *de facto* powers to those of the FSB.

42 Vrist Rønn, K., Diderichsen, A., Hartmann, M. and Hartvigsen, M., eds., 2025. *Intelligence Practices in High-Trust Societies: Scandinavian Exceptionalism?* 1st ed. London: Routledge.

43 Melikhov, A.I., et al., 2020. *Operational and Intelligence Activities of the Law Enforcement Agencies in the System of Ensuring National Security*. IX Baltic Legal Forum 2020, 4.

44 Atlantic Council, 2020. *Lubyanka Federation: How the FSB Determines the Politics and Economics of Russia*. Atlantic Council, 5 October. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/lubyanka-federation/. [Accessed 5 November 2025].

45 Soldatov, A. and Borogan, I., 2022. 'Putin's New Police State: In the Shadow of War, the FSB Embraces Stalin's Methods'. *Foreign Affairs*, 27 July, 3 and 14.

Table 3. Internal Security Services (countries that emerged from the former Soviet Union)

Internal Security Services (former Soviet Union)			
Do not have police powers	Have police/law enforcement powers		
▪ Lithuania ▪ Moldova	▪ Armenia ▪ Azerbaijan ▪ Belarus ▪ Estonia ▪ Georgia	▪ Kazakhstan ▪ Kyrgyzstan ▪ Latvia ▪ Russia ▪ Tajikistan	▪ Turkmenistan ▪ Ukraine ▪ Uzbekistan

For Central Asian states that share its illiberal system of governance, Russia is an important partner and ally. Its intelligence apparatus remains an attractive role model. But one country has rejected this model. Armenia has been gradually working on distancing its intelligence community from the Russian mold. The functions of the Armenian National Security Service, another KGB successor service with close ties to the FSB, have been reduced. It is now primarily a domestic intelligence service. Foreign intelligence responsibilities are being handed over to a separate, newly established organisation with apparently much friendlier ties to Western intelligence services.[46] Its investigation responsibilities for serious crimes related to corruption, smuggling, and narcotics have been transferred to other law enforcement bodies and discussions are also under way to further limit its remaining enforcement powers.[47] Despite its historic ties to Russia, Armenia has shown a remarkable desire to emulate Western governance standards. However, its intelligence reforms will also depend on commitments from its successive governments, as well as the dynamics of a very complex geopolitical environment. Armenia is one of the few post-Soviet states that switched from a strong presidential system of governance to parliamentary democracy.

46 Tuncel, T.K., 2023. 'A New Foreign Intelligence Agency in Armenia'. Center for Eurasian Studies (AVİM), Commentary No. 2023/1, 2 January. Available at: https://avim.org.tr/en/Yorum/A-NEW-FOREIGN-INTELLIGENCE-AGENCY-IN-ARMENIA [Accessed 10 February 2025].

47 Zargarian, R., 2024. 'Armenian Security Service Set to Lose More Powers'. *RFE/RL*, 28 August. Available at: https://www.azatutyun.am/a/33096884.html [Accessed 7 February 2025].

1.1.4. Nexus of intelligence and law enforcement

Imagine that two objects share a confined space—moving about, interacting, and bumping into each other—but each behaves according to its own gravitational forces. Intelligence and law enforcement are like those two objects. They are fundamentally different and often even at odds. Their respective *raison d'etre* and objectives are distinct, as are the ways and means to achieve said objectives. They are simply designed and operate differently. Pursuing their respective missions can easily lead to confrontational standoffs, often requiring higher government officials or judges to intervene. Yet, oftentimes, their interests can also converge or overlap. In some cases, one can become highly dependent on the other, and *vice versa*. Cooperation can be mutually beneficial. But fears of unified intelligence-police powers have led democracy-minded lawmakers to establish 'wall(s) of separation' [48] or 'jurisdictional firewall(s)'[49] between the two. Traversing from indifference to competition to cooperation, their interactions span all the combinatorial trappings of a symbiotic relationship.

The purpose of intelligence is to support national security. Law enforcement, on the other hand, is concerned with supporting justice and public order by enforcing the law. A law enforcement mandate could thus entail investigating (talking to witnesses, questioning suspects, examining data), collecting evidence, arresting suspects (detention), and prosecuting cases. It also entails the coercive use of force. Intelligence is there so information can be collected, interpreted, assessed, and distributed to those authorities that have to act in the best interest of national security. It is 'preventive' in nature, focused on mitigating risks to national security. By contrast, law enforcement is essentially a 'reactive' endeavour, usually triggered by a criminal act. For the police to initiate action there have to be reasonable grounds to believe that a crime has occurred, pursuant to which an investigation can be initiated. Evidence is collected, someone is prosecuted, and a judicial conviction infers a successful ending. While intelligence efforts are predominantly secretive and highly protective of their sources and methods, law enforcement investigations and criminal prosecutions are essentially public endeavours.

Intelligence organisations are ambivalent about being involved in court proceedings. A lot of public information comes out in criminal proceedings, and the risk to national security is often difficult to predict or measure with any great certainty. Whether it is the 'discovery' clause (defendant's right of access to information), special measures, or human sources (secret assets, agents, or collaborators), intelligence organisations would rather not appear in the public eye. Whenever intelligence information enters a criminal case, where the criminal justice and national security systems meet, writes a former senior prosecutor,

48 Manget, F.F., 2006. 'Intelligence and the Criminal Law System'. Stanford Law & Policy Review, 17, 415–436 at 416.

49 Fredman, J.M., 1998. 'Intelligence Agencies, Law Enforcement, and the Prosecution Team'. *Yale Law & Policy Review* 16/2, 331–371 at 331.

'everything gets more difficult'.[50] In 2023, Danish authorities dropped criminal charges against an ex-government minister and a former head of intelligence claiming it was 'in the interest of the state's security', arguing that court proceedings would have depended on classified information, the disclosure of which would have caused damage to national security.[51] Much of the evidence would have come from Denmark's domestic security service PET, authorized to investigate crimes and collect evidence. The high-profile case was controversial from the start, leaving Denmark's intelligence community with irreparable scars. In general, the value of intelligence secrets is independent of both a prosecutor's and defendant's interests, as intelligence organisations are forced to face the inherent risks from criminal discovery and evidentiary rules.[52] A defendant in a trial involving intelligence information might tactically threaten to reveal state secrets ('graymail'), a form of coercion not unlike blackmail. There is little harmony when openness and secrecy clash. But despite the differences, law enforcement and intelligence can also converge.

Public order, justice, and national security are not entirely separate affairs. Traditional threats from spying and a growing array of challenges that go beyond this create unavoidable overlaps. Terrorism, espionage, subversion, cyber-attacks, transnational organised crime, illicit trafficking, and a host of other complex security concerns contribute to a blurring of the line between them.[53] Whether they like it or not, intelligence and law enforcement officials may be forced to cooperate. Terrorist attacks have led some states to establish joint inter-agency centres or specialized task-force units that serve as platforms for cooperation between police and intelligence bodies. Coordinating and sharing information this way reflects the necessary urgency and interdisciplinary tools to respond effectively.

Some offenses, like espionage, collusion, sedition, and subversion, are categorized as crimes against the state or as national security crimes.[54] Disclosing state secrets, attacks on the highest state officials, and acts of terrorism may also apply in some countries. Intelligence services with law enforcement mandates are usually specifically designed and may have exclusive jurisdiction over such offenses. Although treason is the only crime mentioned in the US Constitution, federal laws cover an array of other criminal acts that are considered crimes against the United States. Some countries include 'crimes against the government' within their criminal justice systems. In Russia, state offenses are extensive and greatly fall under 'Crimes Against State Power,' as outlined in Section X of its basic criminal code. Critics have accused Russia of using these and a flurry of newly adopted laws to

50 Aaron, D., 2023. 'I've Prosecuted National Security Cases. It Can Take Time to Get Them Right'. *Just Security*, 19 April.

51 Olsen, J.M., 2023. 'Denmark drops cases against former defense minister and ex-spy chief charged with leaking secrets'. *Associated Press*, 1 November.

52 Manget, 2006. 'Intelligence', 423.

53 Zavrsnik, A., 2013. 'Blurring the Line between Law Enforcement and Intelligence: Sharpening the Gaze of Surveillance?'. *Journal of Contemporary European Research* 9/1, 181–202.

54 Creegan, E., 2012. 'National Security Crime'. *Harvard National Security Journal* 3, 373–430.

legitimize repression and tighten regulations on public protest. The UK recently adopted a new National Security Act focused on domestic threats sponsored by foreign states. The Act was intended to provide police and intelligence services with improved means to respond. In recent years, says a senior UK advisor, we have seen an increase in 'use of organised crime groups' by foreign countries, often 'paying local criminals to carry out acts of violence, espionage and intimidation'.[55] But to the UK's credit, the Act also introduced numerous safeguards, requiring, for instance, the Attorney General's consent for prosecutions and a strong conditionality requirement in proving the involvement of a foreign state.

State threats, unlike common street crimes, can be harder for the public to understand. Offenses against the state are said to generally fall into two categories: conduct against the government and offenses which affect the orderly and just administration of public business.[56] It is naturally difficult to distinguish consistently between legitimate political acts of opposition and attacks on constitutional order. Sometimes, as protests are growing in complexity, there is no clear divide between assemblies that are peaceful and those that are not.[57] But repressive governments are not as concerned about getting the balance right as are democracies. Indeed, authoritarian regimes hardly recognize legitimate political opposition. Democracies, on the other hand, exist because of free speech, civic activism, and the right to organise and protest freely. The purpose of independent oversight and other safeguards is to make sure security services do not target these lawful activities.

The US Department of Justice has a special department for national security. Its mission statement reveals a hidden divide between policing and intelligence work. By stating that the department's role is to protect the country from threats to national security 'by pursuing justice through the law,' it essentially implies having to balance justice and national security. Inherent dilemmas of which interests, justice or security, have primacy are sure to emerge on a case-by-case basis. According to the same mission statement, the department is organised in such a way so as to ensure 'greater coordination and unity of purpose' between prosecutors and law enforcement, on the one hand, and intelligence bodies, on the other. It clearly highlights differences of purpose, as well as the division of labour, that there is between the two. An intelligence mind-set focuses on preventing threats and mitigating risks, as opposed to an evidence-based or criminal law mind-set preparing for the rigors of a courtroom trial. Prosecutors would like to reveal as much information as possible in getting a conviction, while intelligence officials would be far more cautious. As no one has yet invented a way around this impasse, the 'two sides negotiate'.[58]

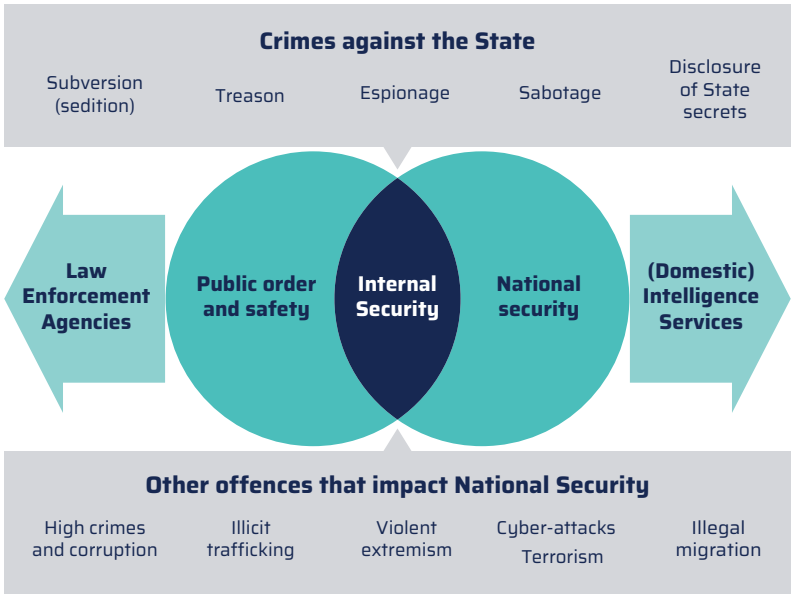
55 Dearden, L. and Landler, M., 2025. 'U.K. Faces "Extraordinary" Threat from Russian and Iranian Plots, Official Warns'. *The New York Times*, 6 June.

56 Packer, H.L., 1962. 'Offenses Against the State'. *The Annals of the American Academy of Political and Social Science* 339/1, 77–89 at 77.

57 Flores, O. 2023. *Case law on peaceful protests*. Global Freedom of Expression, Columbia University, 11.

58 Woodruff Swan, B. and Orden, E., 2023. 'How to hold a public trial when the key evidence is classified'. *POLITICO*, 14 June.

Figure 1. The nexus of justice, public order, and national security



The emerging security environment presents serious challenges of jurisdiction and responsibility. Cyber-attacks represent a case in point. If an attack is orchestrated by cyber criminals with intent to extort financial gains, law enforcement bodies would be expected to respond. On the other hand, if the attack is a state-sponsored effort to access classified information, undermine national sovereignty, or harm other national interests, the intelligence service would likely play a greater role. But often, ascertaining responsibility in cyberspace is no easy task. The intent of the attack could also be difficult to uncover. State actors may be using criminal groups as proxies. And what may start out as a typical cyber-crime investigation could easily evolve into a national security matter. The opposite could also be the case. The FBI has separate departments dealing with criminal and counterespionage investigations. Problems emerge, for example, when the primary purpose of a surveillance operation changes from one to the other, as criminal standards for an effective judicial prosecution clash with a national security rationale.[59] Either way, individual rights and freedoms can easily be infringed as the standards of surveillance authorization vary, and the prospects of arbitrary enforcement become more likely. An intelligence inquiry, sometimes simply to gain better insight and understanding, does not match up standard-wise against the 'probable cause' and other high standard requirements in a criminal investigation.

59 Manget, 2006. 'Intelligence', 417.

The complexities of these and other challenges do not of themselves necessarily suggest it would be better or more beneficial to combine police-intelligence powers into a single organisation. Arguments can be made for having intelligence services with law enforcement powers in democracies: but effective arguments can also be made against. Both options have merit whenever justice and national security interests are aligned. When they're not, as often happens, either variant can still run into serious complications. The only difference would be the nature of the squabble: inter-service or intra-service. The risk of cover-ups and other abuses is, though, it must be acknowledged, greater when concentrating intelligence-police powers under a single authority.

A DCAF study identified three generic prototypes from which any security service derives its mandate in terms of law enforcement.[60] The first model represents intelligence organisations that do not have law enforcement roles or police powers. But it does not mean that domestic intelligence cannot support the police and law enforcement bodies, often with lead information that may be of use to law enforcement bodies. However, the possibility of using intelligence information as evidence in a court of law varies and may depend on a country's statutory regulations. The second model describes services that are mandated to investigate crimes and collect evidence, but usually do not have powers of detention, interrogation or arrest. Without coercive measures, this model may offer a middle ground solution, provided that other key safeguards would be in place. The third model applies to those services with a law enforcement mandate and police powers. These services would usually have jurisdiction over specific crimes, like espionage, terrorism, and/or violent extremism, and would be authorized to undertake pre-trial investigations, collect evidence, and make arrests. The security services of most Western democracies are represented by the first model (no law enforcement mandate), or they fall within a span that consists of elements of the first and second models. It is this nexus between domestic intelligence and law enforcement, writes Lowenthal,[61] that distinguishes Western democracies' version of intelligence from those in totalitarian or authoritarian states.

60 DCAF, 2020. 'Counterintelligence', 2.

61 Lowenthal, 2020. *Intelligence.*

1.1.5. Principles and standards

Advocates of setting standards for internal intelligence services will point to a set of recommendations from the European Commission for Democracy through Law (Venice Commission). Recognizing that internal intelligence services are valuable institutions, the Venice Commission points out the potential hazards of wielding unchecked intelligence powers in a liberal democracy. It highlights traditionally weak public confidence in internal security services, because of the secrecy in which they operate. Unless adequately supervised and without appropriate restraints on its powers, it was argued, internal security services could do more harm than good. Simply put, intelligence services are said to have a deep-seated, inbred potential of abuse of state power. And services having law enforcement powers were particularly worrisome. The Commission believed that the danger stemmed from the services' own inclination 'to act outside the accepted standards of an ordinary police force'.[62]

An institutional separation between intelligence and law enforcement was commonly believed to be a necessary safeguard against abuse, including the risk of the arbitrary use of intelligence information.[63] Separating 'collection (of intelligence information) from enforcement' also acts as a curb on executive decision-making. In the case of New Zealand, it is believed to be an important constitutional check on state power over its citizens and guards against the emergence of a 'secret police'.[64] Nevertheless, institutional separation must never obstruct the necessary cooperation, coordination, and sharing of information between intelligence and law enforcement. On the contrary, we need, according to Arthur Hulnick, to break down the barriers between intelligence agencies and law enforcement.[65] Failing to follow-up on the suspicious behaviour of 9/11 terrorist suspects because they had yet to commit any crimes revealed the need to overcome a system characterized by bureaucratic rivalries and turf battles. An in-house review of the FBI's role found 'inadequate analysis of whether to proceed as a criminal or intelligence investigation'.[66] Despite the tragic consequences of 9/11, calls for better communication and information sharing would trump pleas to unify police and intelligence powers. A few years earlier, a European initiative had attempted to resolve some of these issues.

---

62 Venice Commission, 1998. Internal Security Services in Europe, CDL-INF(98)6. Venice. Available at: https://www.venice.coe.int/webforms/documents/?pdf=CDL-INF(1998)006-e# [Accessed 6 March 2025].

63 FRA – European Union Agency for Fundamental Rights, 2015. *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Mapping Member States' Legal Frameworks*. Luxembourg: Publications Office of the European Union, 28.

64 Cullen, M. and Reddy, P., 2016. *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand*, 29 February.

65 Hulnick, A.S., 2004. *Keeping Us Safe: Secret Intelligence and Homeland Security*. London: Praeger Publishers.

66 US Department of Justice, 2004. 'A Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks', Special Report, Office of the Inspector General (released publicly June 2006).

The Council of Europe's Parliamentary Assembly proposed:

> *'that internal security services should not be allowed to run criminal investigations, arrest or detain people, nor should they be involved in the fight against organised crime, except in very specific cases, when organised crime poses a clear danger to the free order of a democratic state'.*[67]

This was a milestone moment, a benchmark for old and new democracies alike, although more likely intended for the latter. It is a good rule that intelligence and law enforcement be separate, concluded a working group of experts, as their purposes are fundamentally different.[68] Police enforcement powers of arrest, interrogation, and detention in combination with a security service's special measures creates a potentially powerful and excessively influential institution. Using intelligence information to manipulate and put pressure on individuals was bad enough. But buttressed with the threat of arrest or criminal prosecution, it was a disreputable tool of intimidation against opponents in communist regimes. Little had changed according to *The Economist*: 'It is hard to find an ex-communist country in eastern Europe in which the intelligence and security services are depoliticized and uncontroversial.'[69] Intelligence reforms would prove to be slow and limited. Despite preferences for separating intelligence and law enforcement, international experts would eventually begin to relax their previously held views. But they would not do so unconditionally.

Intelligence services with law enforcement powers are acceptable in a democratic system of government if certain standards were met.[70] Accountability, the protection of individual rights, and guardrails against abuse of powers would have to be assured. Such services would have to be under tight internal and external (independent prosecutor) control, as well as having their investigative special measures subjugated to appropriate approval. The 'probable cause' requirement for initiating surveillance and searches would have to go through an independent review by a neutral and detached judge issuing a specifically limited warrant.[71] Any law enforcement responsibilities and powers of security services would have to be clearly enshrined in public law.[72] Overlapping mandates and enforcement

---

67 Council of Europe, Parliamentary Assembly, 1999. *Control of Internal Security Services in Council of Europe Member States, Recommendation 1402*, April. Available at: https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16689&lang=en [Accessed 20 January 2025].

68 DCAF, 2003. *Intelligence Practice and Democratic Oversight – A Practitioner's View*, Occasional Paper No. 3. Geneva: DCAF, 31.

69 *The Economist*, 2006. 'Spy scandals in eastern Europe reveal some damaging hang-ups', 19 December.

70 Venice Commission, 2007. *Report on the Democratic Oversight of the Security Services*, CDL-AD(2007)016. Venice, 1–2 June, 21.

71 Cooperstein, T., 1997. 'The Emerging Interplay Between Law Enforcement and Intelligence Gathering'. *International and National Security Law Practice Group Newsletter*, 1/3.

72 DCAF, 2011. Compilation of Good Practices for Intelligence Agencies and Their Oversight. Geneva: DCAF. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/International_Standards_Eng_23-10.pdf [Accessed 20 March 2025], 26.

powers with the police would have to be avoided. For instance, if an existing police organisation has jurisdiction over investigating and prosecuting a particular crime, there would be no need for the security service to do so as well. The US Foreign Intelligence Surveillance Act (FISA) provides some insight in how intelligence gathering and narrowly focused criminal targeting (especially when it intersects with national security) can be balanced.

International standards on police powers would also apply. Intelligence service officials exercising police powers are bound by the Code of Conduct for Law Enforcement Officials, adopted by the UN General Assembly resolution 34/169 on 17 December 1979. In using its police powers—including arrest, interrogation, and detention—the service should comply with the same standards as those of law enforcement agencies, respecting human rights, due process, and right to a fair trial. Other enforcement principles like requiring 'reasonable suspicion' and prohibiting 'arbitrary' arrest or detention would also have to be respected. Furthermore, it would be unacceptable to use these coercive powers as instruments in collecting intelligence. As a good rule of thumb, the same legal protections for individual privacy should exist regardless of whether evidence implicating an individual in a crime came from an intelligence or law enforcement body.[73] And the intelligence service would need to be subjected to the same level of oversight and judicial review in relation to the lawfulness of their conduct.[74]

Cross-over investigation cases pose serious challenges. Judges approving surveillance warrants and oversight bodies reviewing the use of special measures would have to be especially vigilant. For example, what happens if an intelligence operation turns into a criminal investigation (or the other way around)? But what if that was the intent in the first place? The risks of abuse are certainly greater when there are no institutional walls between the two. Allegations of Russian interference in US elections resulted in controversy when a US special counsel counterintelligence-focused probe later turned into an investigation of criminal wrongdoing.[75]

73 Mannes, A.B., 2017. 'Law enforcement and intelligence agencies are not synonymous'. *The Hill*, 28 April.

74 DCAF, 2011. *Compilation,* 26.

75 Zebley, A., Quarles, J. and Goldstein, A., 2024. *Interference: The Inside Story of Trump, Russia, and the Mueller Investigation*. New York: Simon & Schuster.

1.1.6. Challenges of intelligence-law enforcement merger

The challenge in managing intelligence and law enforcement in a single institution stems from their inherently fundamental differences, including the diverging worldviews discussed earlier. The first hurdle to overcome is effectively balancing their competing objectives. The second involves dealing with issues in which the two overlap or share common threats. The third arises from concerns over misapplication of powers stemming from their mandates being fused. While the first two challenges are common to other administrative, functional, or institutional mergers, concerns of misapplication of powers are central to good governance, especially when individual rights and the rule of law are at stake.

Intelligence, be it foreign or domestic, is inextricably couched in a national security context. But national security is a vague and mercurial term. Understandings of national security have fluctuated even over the last couple of decades. Correspondingly, lawmakers find it so contentious that they avoid defining it in formal legislation. There is no legal definition within the EU or even a common understanding among its member states.[76] Even scholars have found national security difficult to harness, much less reach consensus on its meaning, finding it stretched almost beyond recognition.[77] In the 'Esbester v. the UK' case, the European Commission of Human Rights finds that interpretation and application of 'national security' are matters of practice, ruling that a comprehensive definition was not even possible. It is this fuzziness and inherent legal uncertainty that often proves incompatible with the 'rule of law' standards of law enforcement and the justice system.[78]

European case law provides some insight: though these insights are far from the kind of clarity that legal systems are used to. EU treaty law sets national security as the responsibility of each member state. As a result, member states have had significant discretion in identifying threats and in deciding how to respond. In the past, states were given an almost unrestrained 'margin of appreciation' (space for manoeuvre on national security issues *vis-à-vis* human rights). That has gradually changed. In some cases, any room for manoeuvre is now explicitly excluded and in others it has been reduced; the member state's 'margin of appreciation' in national security cases in general is no longer considered uniformly broad.[79] Thus, what used to be an untouchable 'national security exemption' has become a subject of great debate, not least as it relates to classified information and intelligence

76 Nowinski, M., 2022. 'National Security Clause in the EU Law and Its Implications for Intelligence and Security Services'. In: P. Burczaniuk, ed. *Legal Aspects of the European Intelligence Services' Activities. Warsaw: Internal Security Agency* (Poland), 273–290 at 273.

77 Drezner, D.W., 2024. 'How Everything Became National Security'. Foreign Affairs, 103/5, September/October, 122–135 at 123 and 135.

78 European Parliament, 2014. *National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges, Study for the LIBE Committee, Directorate-General for Internal Policies*, PE 509.991. Brussels: European Union, 7.

79 European Court of Human Rights, 2013. National Security and European Case-Law, Research Division Report, 40.

activities. In that context, the Court of Justice of the EU has ruled that exceptions to fundamental rights and freedoms must be justified and interpreted narrowly, highlighting the applicability of EU law despite the traditionally weighty concerns of state security.[80]

A national security pretext has been exploited by governments to justify some of the most serious violations of the rule of law and fundamental rights and freedoms.[81] Protecting a government from embarrassment or exposure of its corruption cannot be equally justifiable as protecting a country's sovereignty or its territorial integrity.[82] Indeed, the danger of manipulation and political abuse is very real. For this reason alone, democracies are well aware of the need for proper control, oversight, and accountability. Risks can be further mitigated by establishing proper checks and balances between the main power brokers. Concerns are rightfully raised when intelligence and law enforcement powers are brought together in a single service. But it can be just as worrisome when intelligence services provide support to police investigators, as pointed out in the next paragraph. Independent oversight and other safeguards against abuse can play a key role.

Side-stepping procedural norms, by indiscriminately using measures from a mixed toolbox of police and intelligence capabilities, undermines the rule of law and can violate rights. Evidence could easily be rendered useless in court proceedings if it was not obtained under tight legal protocols. Law enforcement investigators have been known to conceal the origin of information derived from intelligence surveillance operations. By claiming the information as their own and using it in criminal proceedings, critics say these national authorities are engaged in 'intelligence laundering'.[83] Section 16 of New Zealand's Security and Intelligence Act specifically prohibits its intelligence service NZSIS from undertaking any enforcement measures. A New Zealand intelligence review board emphasized that there was no justification for the use of intelligence capabilities in law enforcement beyond what the police can do lawfully.[84] When assisting the police, according to the same review, intelligence capabilities cannot be used to detect crime at an early stage.[85] Alternatively, domestic intelligence operatives run into problems when citizens, exercising their rights, are unwilling to voluntarily cooperate. The surgical use of police powers may, in these circumstances, come in handy. 'If a cop

80 FRA – European Union Agency for Fundamental Rights, 2015. *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Mapping Member States' Legal Frameworks*. Luxembourg: Publications Office of the European Union, 10. That the national security exemption cannot be seen as entirely excluding the applicability of EU law was reaffirmed in FRA's 2023 update *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU – 2023 Update*, 7.

81 Article 19, 1996. The Johannesburg Principles on National Security, Freedom of Expression and Access to Information. London: Article 19, 6.

82 Article 19, 1996. 8.

83 Farrow, R., 2020. 'How a CIA Coverup Targeted a Whistle-blower'. *The New Yorker*, 30 October.

84 Cullen and Reddy, 2016. *Intelligence and Security*, 236.

85 Cullen and Reddy, 2016.

follows you for 500 miles,' claimed Warren Buffett, 'you're going to get a ticket.'[86] Buffet was referring to a fellow investor who had been under investigation for quite some time before finally being penalized. Intelligence officials might be tempted to use the same tactics and threaten individuals with criminal prosecution in order to access information or push someone into coerced collaboration.

Evading or violating procedural constraints, however minor at first, eventually results in systemic decay. Police officers, wanting to put the 'bad guys' behind bars, may be tempted to break a few minor rules. Restraint in wielding authority does not come naturally to those in power. Crime fighters and secret agents are easily drawn to 'noble cause' ethical dilemmas. Also referred to as 'noble cause corruption', it means to morally justify using illegal or unethical means in order to reach utilitarian ambitions. It amounts to convincing oneself of achieving a good greater than the harm caused by any wrongdoing. Although the concept is rooted in theological ethics, it applies as well to those serving to protect the nation. Security services in particular have often done the government's 'dirty work', be it to shield the regime or working in what they consider the nation's best interests, acting, in either case as if they were above the law. The United Nations Human Rights Committee urged the Turkish government to consider overturning provisions in a law that grants extensive immunity to intelligence agents from criminal prosecution.[87] Such privileges openly promote a culture of impunity among intelligence operatives. A democratic society cannot afford to allow any individual or authority to be above the law.[88] Napoleon's famous maxim 'he who saves his country does not violate any law,' has been posted in February 2025 by a head of state. A devil's advocate promoting a 'noble cause' principle could not have asked for a better endorsement.

Police-intelligence powers, when supplemented with tailor-made laws that target political opponents and unjustly restrict rights and freedoms, can lead to more widespread, systemic abuses. A flurry of laws has further accelerated Russia's slide back to Soviet-era tactics designed to curb dissent.[89] The most recent, dubbed the law on so-called 'undesirable organisations', is intended to provide justification for taking action against critics of Russia's war in Ukraine. Organisations and individuals can be targeted if their activities pose a threat to the constitutional order, defence or state security.[90] It seems perfectly well suited for the FSB's already controversial law enforcement powers. The law's vagueness and flexibility enables Russia's enforcement bodies to exercise extensive discretionary powers. Countless bans, fines, arrests, and criminal prosecutions have been instigated. More so,

86 Crippen, A., 2013. 'Buffett on JPMorgan: Jamie Dimon will survive fine'. *CNBC*, 16 October. Available at: https://www.cnbc.com/2013/10/16/buffett-on-jpmorgan-jamie-dimon-will-survive-fine.html [Accessed 6 April 2025].

87 UNHRC – United Nations Human Rights Committee, 2024. *Concluding observations on the second periodic report of Türkiye: Adopted by the Committee at its 142nd session* (14 October – 7 November), 5.

88 Venice Commission, 1998. *Internal Security Services*, 17.

89 Litvinova, D., 2024. 'How Putin's crackdown on dissent became the hallmark of the Russian leader's 24 years in power'. *Associated Press*, 6 March.

90 Rescheto, J., 2024. 'Russia tightens "undesirable organisations" law'. *Deutsche Welle*, 27 July.

its effectiveness has been in the fear it instils among the general population. In a similar fashion, China imposed a controversial national security law on Hong Kong intended to quell public unrest and suppress political opposition. While the law lays out secession, subversion, terrorism, and collusion as punishable acts (including life sentences), critics say the law also serves to stamp out pro-democracy and human rights groups, independent media, and external interference. Russian and Chinese intelligence services play by fundamentally different rules from those of their Western counterparts; neither one is subject to the rule of law or to independent oversight; nor are they scrutinized by a free press or held publicly accountable; in fact, one analyst argues, both are 'limited only by operational effectiveness—what they can get away with'.[91]

Serbia's Security-Intelligence Agency (BIA) stands out among the countries that emerged from the break-up of the former Yugoslavia. Of the six, or seven if you include Kosovo, BIA is the only regional intelligence service with a law enforcement mandate and police powers. Not only does BIA enjoy the full spectrum of police powers, BIA also has exceptional influence and jurisdictional pre-eminence over law enforcement bodies. According to Article 16 of the Law on the Security-Intelligence Agency, in circumstances deemed in the interest of state security, BIA may take over and directly process cases that would otherwise be the responsibility of the police. Likewise, Serbia's covert communication interception facility is located within BIA, giving the intelligence service a bird's-eye view of all police investigations.[92] Accusations of abuse and political manipulation have led many critics to scrutinize BIA's law enforcement powers.[93] In 2023, Serbia's EU progress report called on the government to reconsider BIA's role in criminal proceedings. More specifically it called for an end to using security services in criminal proceedings altogether or, at least, asked that such cases be limited to exceptional cases of communication interception.[94] The EU also called for a clear separation between criminal investigations and those for security purposes.[95]

91 Walton, C., 2023. 'The New Spy Wars: How China and Russia Use Intelligence Agencies to Undermine America'. *Foreign Affairs*, 19 July.

92 Petrović, P., 2020. *The Security Information Agency: The Anatomy of Capturing Serbia's Security-Intelligence Sector*. Belgrade: Belgrade Centre for Security Policy, 26.

93 Guilbert, K., 2024. 'Serbia used spyware to hack phones of journalists and activists, Amnesty says'. *Euronews* 16 December; Petrović, P., 2021. 'State Capture and Security Intelligence Agencies in Serbia'. *Journal of Regional Security* 16/2, 151–182.

94 European Commission, 2023. *Serbia 2023 Report: 2023 Communication on EU Enlargement Policy*, SWD(2023) 695 final. Brussels. Available at: https://enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_695_Serbia.pdf [Accessed 22 February 2025], 54.

95 European Commission, 2023. *Serbia Report*.

1.1.7. Conclusion

Intelligence services are not well suited to exercising law enforcement powers in a modern democracy, which is not to say they cannot lawfully provide support to and cooperate with the police or law enforcement bodies. Undemocratic governments are prone to relying on security services, vested with extensive law enforcement authority, as instruments of political repression.[96] Nevertheless, some vibrant democracies have chosen to maintain security services with law enforcement mandates, albeit with clearly defined powers, effective executive control, independent oversight and safeguards against political and human rights abuse. A proven culture of accountability is also necessary. Nordic countries are a good example here. With high levels of societal trust, traditional security practices, and modestly sized services, a Scandinavian context may be exceptional.[97]

Post-authoritarian societies are particularly vulnerable and should take extra precautions. Removing law enforcement powers can contribute to greater public confidence in the intelligence community (as in the Croatia case study). This is especially important because of the need to operate in secrecy. EU candidate countries that have yet to separate law enforcement powers from their security services have been encouraged to do so. Countries with authoritarian legacies in which security services violated fundamental rights and freedoms should be especially wary. Lord Acton's proverbial warning that 'power tends to corrupt and absolute power corrupts absolutely' resonates well in this instance. More specifically, Acton warns us that the more power someone holds, the more judgmental we should be of their actions. Intelligence services with law enforcement mandates surely require preponderant vigilance and should be subject to even greater scrutiny than those services without police or law enforcement powers.

96 DCAF, 2017. 'Intelligence Services: Roles and responsibilities in good security sector governance', SSR Backgrounder Series, 1 September. Geneva: DCAF. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_12_IntelligenceServices_EN_Jul2022.pdf [Accessed 11 February 2025], 4.

97 Vrist Rønn, K., et al., 2025. *Intelligence Practices*, 2.

Part II: The oversight and accountability mechanisms for intelligence services including those with law enforcement functions

Effective democratic governance of intelligence services, particularly those vested with law enforcement powers, depends on robust oversight and accountability mechanisms. Among these, parliamentary oversight is often regarded as the cornerstone. Parliaments, as the elected representatives of the people, have the authority and legitimacy to scrutinise intelligence activities, review budgets, assess compliance with the law, and investigate abuse allegations. Parliamentary committees and commissions can compel testimony, request documents, and hold hearings, thereby ensuring that intelligence agencies operate within their mandates and under the rule of law.

Yet, while parliamentary scrutiny is indispensable, it is not enough. Intelligence work is, by nature, secretive, technically complex, and fast-moving, which can limit parliamentary capacity to monitor all activities in real time. This is why additional layers of oversight are essential in providing a comprehensive accountability system. Judicial oversight through courts, warrant procedures, and review of intelligence-led operations ensures that intrusive measures respect fundamental rights and meet tests of legality, necessity, and proportionality. Executive supervision provides strategic direction, allocates resources, and aligns intelligence priorities with national policy. Independent bodies, meanwhile, such as inspectors-general and ombudspersons investigate complaints, review compliance, and serve as accessible channels for individuals whose rights may have been infringed.

Beyond state institutions, civil society organisations, the media, and whistleblowers play a crucial role in shedding light on misconduct, exposing unlawful practices, and stimulating public debate about the appropriate limits of state secrecy. Responsible investigative journalism can prompt formal inquiries and reforms, while rights-focused NGOs contribute expertise, legal action, and public advocacy.

Taken together, these complementary mechanisms create a multi-layered system of oversight that helps protect democratic values, uphold the rule of law, and maintain public trust in the sensitive but vital work of intelligence services.

2.1. Ensuring legislative scrutiny: Parliamentary powers

Teodora Fuior

2.1.1. Intelligence oversight and its challenges

By parliamentary oversight we refer to the continuous monitoring, review, and evaluation of government and public agency activities, including policy implementation, legislation, and public spending. Parliamentary oversight is a cornerstone of the separation of powers and a fundamental pillar of democracy.

Intelligence oversight is a relatively recent and complex parliamentary responsibility. Historically, national security and intelligence were seen as exclusive domains of the executive, with legislatures and courts largely abstaining. Since the end of the Cold War, however, the parliamentary oversight of intelligence has become a democratic norm, driven by three core goals:

- Preventing political abuse of intelligence services while enabling effective executive management;
- Upholding the rule of law by ensuring intelligence activities comply with legal standards and respect democratic values, including human rights;
- Ensuring public funds allocated to intelligence are used efficiently and as approved by parliament.

The complexity of the intelligence community presents a significant oversight challenge. Intelligence functions are diverse and spread across autonomous agencies and ministries. Most countries have—alongside specialized units handling crime, cybersecurity, or national protection—three primary intelligence types: domestic, foreign, and military. These mandates increasingly overlap and blur.

A defining characteristic of intelligence services is the **secrecy** of their operations and their use of intrusive powers that affect fundamental rights, especially privacy. Examples include communications interception, covert surveillance, property intrusion, hacking, and undercover operations using false identities.

Box 1. What are the typical challenges in the parliamentary oversight of intelligence?

Secrecy: Oversight is complicated by the confidential nature of intelligence work and the discretionary authority of officers. Effective oversight requires access to classified information, expertise, and time. Independent oversight bodies with clear mandates can help address this.

Insufficient political will: Oversight of secret activities offers little public visibility or political gain. This may discourage elected officials from engaging actively.

Exaggerated threat perceptions: National security threats can be overstated to justify disproportionate actions. Professional, independent oversight is essential in ensuring that intelligence analysis does not over – or under-estimate the severity of a threat to national security.

Increased international cooperation: The secret nature of intelligence work applies in particular to international cooperation, which is often beyond the reach of national oversight bodies who are limited to national jurisdiction. This is raising risks of abuse—as shown in scandals such as the Snowden revelations on mass surveillance or secret detentions. Defining clear rules for international cooperation helps prevent misconduct.[98]

Rapid technological change: Oversight often lags behind the fast pace of technological innovation. Updating legal frameworks and involving technical experts is critical for closing accountability gaps.

Ensuring accountability for intelligence services that combine intelligence gathering with law enforcement powers presents additional challenges. These agencies often operate with broad authority, including surveillance, infiltration, search and seizure, arrest powers, and covert operations. These are typically justified by the urgency of addressing threats like terrorism, espionage, or cyberattacks.

Granting law enforcement powers to intelligence services can improve a state's capacity to respond swiftly and effectively to such complex threats. It enhances information sharing, operational coordination, and enables more proactive interventions. It may also allow intelligence to be used as admissible evidence in court, bridging the gap between threat detection and prosecution.

98 For a review of challenges brought by international cooperation and good practices in their oversight see Born, H., Leigh, I. and Willis, A., 2015. *Making International Intelligence Cooperation Accountable*: DCAF and EOS. Available at: https://www.dcaf.ch/making-international-intelligence-cooperation-accountable [Accessed 17 October 2025].

However, the fusion of intelligence and law enforcement functions significantly increases the risk of abuse, especially in environments with weak or politicized oversight. Preventive intelligence operations and criminal investigations are governed by different legal standards: the first often allows for action based on lower thresholds of suspicion and fewer safeguards; while the second demands strict legal protections to uphold individual rights.

When intelligence agencies conduct coercive operations without clear legal boundaries, judicial oversight, or transparent accountability, they risk violating fundamental rights to privacy, expression, association, and due process. These violations are difficult to uncover and address, placing greater pressure on oversight bodies to monitor conduct effectively. Over time, real or perceived abuse by secretive agencies acting as internal security forces can seriously erode public trust in democratic institutions. Thus, the very tools meant to protect national security can undermine said security and damage the legitimacy of state authority.

Box 2. What further challenges arise when overseeing intelligence services that possess law enforcement power?

Dealing with a fragmented legal framework: Unlike traditional intelligence services which are usually governed by a single statute, these hybrid bodies are subject to overlapping laws—on national security, policing, surveillance, and criminal procedure. These can obscure lines of responsibility and limit oversight bodies' ability to assess legality and compliance.

Erosion of legal safeguards and accountability gaps: Intelligence operations are typically covert and preventive, operating under lower standards of proof and with limited public scrutiny. Law enforcement, by contrast, acts reactively, within a strict legal framework designed to protect individual rights and to ensure due process. When intelligence agencies are allowed to operate like police without adapting to the same procedural guarantees, there is a real risk of unlawful surveillance, arbitrary detention, and the use of intelligence as unchallengeable evidence in court. Blurring the roles of intelligence and police can lead to turf wars, duplication of efforts, unclear jurisdiction and accountability gaps, where no agency takes responsibility for abuses. Parliamentary bodies must ensure mandates are clearly defined and consistently followed.

Need for granular oversight: Oversight cannot remain purely political or strategic. When intelligence agencies carry out arrests, searches, or interrogations, parliaments must scrutinize operational decisions and individual cases to detect the misuse of power or rights violations. This shift requires increased access to sensitive information and stronger investigative capacities, which most parliamentary committees are not traditionally equipped for.

Dependence on other oversight actors: Even more than in intelligence oversight, parliamentary committees cannot provide effective control on their own. They must coordinate with judicial bodies (for authorizing intrusive measures), independent oversight institutions, data protection authorities, and complaints mechanisms. Internal control mechanisms within intelligence agencies—such as Inspectors General (IGs)—are critical for ensuring the accountability and upholding the rule of law.[99] These mechanisms are often more effective than external oversight alone, as they operate from within and have direct access to sensitive information. Without this multi-actor collaboration, critical aspects of accountability—especially for covert or coercive actions—remain unchecked.

Increased risk of politicisation and abuse: When oversight is weak or co-opted, intelligence agencies with policing powers may be used to silence opposition, target journalists, or harass civil society. Without strict legal boundaries, they can become a tool of regime protection rather than national security. Parliamentary oversight is essential to prevent this kind of abuse, but it is often the first mechanism to be sidelined in politicized environments.

Parliamentary oversight of intelligence services with law enforcement powers is not just a technical necessity: it is a democratic imperative. Without robust oversight, these agencies can become powerful instruments of political control and repression. Legislators must recognize the high stakes involved and assert the role of parliament in defending the rule of law, individual rights, and democratic accountability in the intelligence sector.

2.1.2. Levels of action in parliamentary oversight

Parliamentary oversight starts with the legislature's power to make laws and approve government policies, and continues through regular scrutiny of their implementation. This allows members of parliament to identify flaws in legislation, poor administration, abuses, or corruption. Oversight is a responsibility of the entire parliament, carried out at three complementary levels: plenary sessions, committees, and individual actions by members.

99 For example, in the United States, the CIA's Inspector General must immediately report any identified wrongdoing to the two congressional intelligence committees; the IG is required to appear regularly before these committees to provide updates on their activities and findings. This framework exemplifies how a legislative body can develop innovative mechanisms to maintain insight and oversight over highly secretive institutions.

Box 3. What are the levels of action in parliamentary oversight?

Plenary session	▪ Endorse security strategy and government's policy. ▪ Enact laws. ▪ Approve the use of public funds (State Budget Law). ▪ Debate and decide on motions and votes of confidence. ▪ Consent to top appointments (ministers, intelligence directors).
Committees	▪ Issue reports and formal opinions on draft legislation. ▪ Conduct hearings, visits and inspections in the field. ▪ Undertake inquiries (most soften pending on approval in parliament). ▪ Investigate citizens' complaints. ▪ Issue oversight reports which instigate debate in the plenary. ▪ Issue recommendations for accountable insstitutions. ▪ May hear and provide an opinion on candidates for intelligence directors.
Members of Parliament, individually	▪ Propose new bills and legislative amendments. ▪ Address formal questions and interpellations to the executive (in the plenary, oral or written). ▪ Submit requests for information (free or classified).

The plenary session is the most visible scene of parliamentary work and a key venue for shaping policy. It is where laws are passed, government actions evaluated, and major political declarations made. All binding parliamentary decisions are debated and voted on in plenary. In the security field, parliaments may debate and approve key strategic documents which guide long-term national security policy: such as the Government Program,[100] National Security Strategy, Defence Review, or White Papers on Defence. These documents set priorities for security agencies, including defence spending,[101] personnel limits, arms acquisition, and international deployments. While intelligence services may not be explicitly mentioned, such documents shape their role and position within the broader security sector. However, plenary sessions are rarely suited for intelligence oversight, as they often lack the discretion and expertise needed in such sensitive matters.

Oversight is most effectively carried out at the committee level. A well-structured system of standing committees, aligned with government ministries, is essential

100 The Government Program's approval in parliament is typical in parliamentary systems.

101 Usually as a percentage of Gross Domestic Product.

for a functional and influential parliament. Strong committees operate with independence and are key to both shaping policy and holding the executive accountable. Committees review and advise on legislation and parliamentary decisions within their areas of focus. Their reports form the basis for plenary debates and often guide government action. Committees hold executive agencies accountable in two main ways:

- **Administratively:** by ensuring policies comply with the law, protect citizens' rights, and prevent mismanagement or corruption.
- **Politically:** by assessing whether government decisions align with national interests, the approved government program, and their actual outcomes.

2.1.3. Committees mandated to oversee intelligence

Intelligence oversight is the newest area of parliamentary scrutiny, marked by secrecy, national specificity, and diverse institutional models. No other field of parliamentary oversight varies as widely across Europe. There are three approaches in setting up intelligence oversight, evolving towards increased specialization and organisational complexity:

- Defence and security committees
- Dedicated intelligence oversight committees
- Expert oversight bodies

The first two are now present in all EU parliaments. Expert bodies, by contrast, operate outside parliament; their members are not MPs but are appointed by and report to parliament. The following section will examine the features and comparative advantages of each model.

2.1.4. Defence and security committees

These standing committees have a broad mandate, dealing with legislation and oversight for the whole security sector, including the Ministries of Defence and Interior, law enforcement agencies, intelligence services. A decade or two ago, in most consolidated democracies and transitioning countries, this was the sole committee dealing with all security and intelligence issues. Today, this is the case only in a few countries with relatively small security sectors, such as Albania, Moldova and Montenegro.

Given their broad mandates, defence and security committees often provide only limited oversight of intelligence agencies. With numerous responsibilities, limited time, and often lacking access to classified information and specialized expertise, they tend to prioritize more publicly visible issues. Some adopt sub-committees

to focus on specific institutions or topics (such as intelligence oversight), which can improve focus and reporting. However, sub-committees are often low impact, suffering from limited size, low visibility, and weak institutional support.

Despite these challenges, broad-mandate committees offer the advantage of a holistic understanding of the security sector, which is especially useful for overseeing intelligence with a law enforcement mandate. Their integrated view helps align legislation and oversight across institutions.

In addition to defence and security committees, other parliamentary bodies—such as those on justice, human rights, law enforcement, or public finance—may oversee aspects of intelligence work, either through specific mandates or ad-hoc reviews. Budget and public accounts committees, in particular, are responsible for reviewing the finances of ministries and autonomous intelligence agencies.

2.1.5. Intelligence oversight committees

Most European parliaments have established dedicated intelligence oversight committees to complement their broader defence and security committees. In comparison, they have a narrower and more **focused mandate**, which allows members and staff to develop specialized expertise and concentrate resources on oversight. In many parliaments, the defence committee continues to lead on legislation related to intelligence, while the oversight committee focuses on monitoring operations and ensuring accountability.

To enhance legitimacy, these committees are often joint bodies composed of members from both houses of parliament (e.g. Bosnia and Herzegovina, Romania), and the opposition plays a key role, frequently holding the chairmanship (e.g. Italy, Serbia) or even a majority of seats (e.g. Slovenia).

There are two main models for defining their mandates:

- **Functional approach:** One committee oversees all intelligence functions, regardless of which agency performs them. Some parliaments add specialized bodies to review intrusive surveillance powers. For instance, Bulgaria and North Macedonia have separate committees for communications interception; Germany's G10 Commission plays a similar role.

- **Institutional approach:** Separate committees are assigned to specific intelligence services (e.g. Czechia, Romania, Slovakia). This allows for deeper specialization but can risk fragmentation if multiple committees divide responsibilities without coordination.

Intelligence oversight committees are often established with a **stronger legal basis** than other parliamentary bodies. Their mandates and powers may be defined in a special law for the parliamentary oversight of intelligence (e.g. Germany, Italy, Slovenia, Spain), through a parliamentary decision describing their mandate and powers (e.g. Poland, Romania), or detailed parliament rules of procedure (e.g. the Netherlands). In some cases, their existence is even constitutionally mandated (e.g. Germany), and they may be required to adopt their own rules of procedure (e.g. North Macedonia and Romania).

Box 4. Who is responsible for intelligence oversight?

	Defence and security committee	Intelligence oversight committee	Expert body (extra-parliamentary)
	Albania, Lithuania, Moldova, Montenegro.	Bosnia Herzegovina, Czechia, Denmark, Finland, France, Hungary, Latvia, North Macedonia, Poland, Romania, Spain, and the US.	**Belgium** (Committee I), **Norway** (EOS) **Finland** and **Lithuania**, (intelligence oversight ombudsman), **Netherlands** (Review Committee on Intelligence and security Services), **Portugal** (Council for the Oversight of the Intelligence System), **Switzerland** (independent supervisory authority for intelligence activities).

Characteristics			
Members	Proportional representation of major parliamentsry groups.	Smaller number of members than other committees. Proportional representation, guaranteed participation of opposition/ minority parties. Sometimes government or parliament leaders have a role in appointments.	Respected, senior figures, former politicians or judges, civil society representatives No current allegiance to political parties Appointed by parliament.
Chairmanship	Majority, usually.	Opposition, usually.	Elected by members-
Legal base	Weak. Parliamentary rules of procedure.	Strong. Special law or parliament decision, own rules of procedure.	Special law, own rules of procedure.
Mandate	Wide: all/most of security sector. Legislation and all aspects of oversight.	Narrow: few intelligence agencies. Oversight only; legality, human rights, budget, closed operations.	Narrow: few intelligence agencies. Oversight only; legality, human rights, closed operations.
Access to information	Most often granted without vetting. Staff always vetted	Granted after a secrecy oath in the beginning of the mandate; sometimes conditioned by security clearance. Staff always vetted.	Members and staff are vetted and get security clearance.

Expertise and support staff	General: Thorough understanding of the security sector.	Focused: In-depth understanding of intelligence sector.	Focused: Strong secretariat and expert support (ex. 13 in Norway, 25 in Belgium).
Advantages	Comprehensive expertise, good integration of legislative and oversight functions.	Democratic legitimacy. In-depth understanding of intelligence, expertise. Good use of time and parliamentary resources.	Independence, expertise. Effective oversight: full time and expertise invested in the job. Gain the trust and respect of intel community. Produce informative reports on intel.
Disadvantages	Lack of time and interest in focusing on intelligence Lenient to intelligence services and government, when led by a non-vigilant majority.	Risk missing the big picture. Their expertise is not fully used in legislative procedure when legislation stays with the defence committee. Politicization: when opposition leads oversight there is a risk of exacerbated political strife undermining effective oversight.	Lack of legitimacy. No legislative function. Rarely has authority to control budget execution.

Intelligence oversight committees offer several advantages that support effective and democratic control of intelligence agencies. Their clear legal foundation and narrow, focused mandate promote the development of specialized expertise and efficient oversight procedures. One of their key strengths is democratic legitimacy: they are composed of elected representatives, with opposition parties often playing a prominent role (holding the chair or a majority of seats). This cross-party structure helps ensure that intelligence services serve national interests rather than those of a ruling party.

These committees can influence intelligence agencies through various parliamentary tools, including budget control, legal reforms, public pressure, and personnel decisions. Their findings and recommendations typically require a response from the executive and the agencies concerned.

However, several challenges limit their effectiveness. Politicization is a major concern. MPs may prioritize party interests over objective oversight. Government party members may avoid exposing sensitive issues, while opposition MPs might use the committee platform for political gain. In volatile or polarized political contexts, especially with populist parties on the scene, there is also a greater risk of information leaks for political advantage.

Another limitation is the lack of time and expertise. MPs often serve on multiple committees and must divide their attention between legislative work, constituency duties, and party responsibilities. As a result, oversight committees may meet infrequently: sometimes as little as once a month. Members often lack the technical background to fully grasp intelligence operations. Frequent turnover due to elections or party reshuffling further hinders the development of institutional knowledge within the committee.

A carefully selected, well-educated, and impartial professional staff is essential for effective intelligence oversight committees. These experts carry out the demanding day-to-day work of gathering information, analysing agency conduct, and monitoring compliance with legal and democratic standards. Their insights and diligence enable them to identify issues early and to provide parliamentarians with the information and guidance needed to take appropriate action. Without a strong backbone of professional support, even the most committed oversight bodies may struggle to fulfil their mandate.

Box 5. Examples of intelligence oversight committees

United States Permanent Select Committees on Intelligence (one in the House, one in the Senate)[102]

- Oversee eighteen agencies, the entire intelligence community (functional approach).
- Established in 1976 (Senate) and 1977 (House of Representatives), after a one-year parliamentary investigation in abuses by CIA, NSA, FBI (Church Committee).
- Members appointed by House (22) and Senate (fifteen) leaders.
- Mandate: legislation, budget, legality and effectiveness, operations, top intelligence appointments.
- Powers: subpoena, full access to information and sites, authorize covert operations.
- Foreign Surveillance Act 1978 creates FISA Court—specialized court authorises use of secret surveillance.
- Intelligence Oversight Act 1980 requires prior notice of Congress for all important operations: ensured by the Gang of Eight – bi-partisan group of leaders in Congress who are briefed on top classified intelligence operations.[103]
- Committees meet roughly twice a week for 1½ to 2 hours, generally in closed session.
- Have their own Rules of procedure: https://www.intelligence.senate.gov/about/rules-procedure; https://docs.house.gov/meetings/IG/IG00/CPRT-116-HPRT-IG00-CommitteeRules.pdf
- Relevant subcommittees: United States House Intelligence Subcommittee on Defense Intelligence and Warfighter Support.

German Parliamentary Control Panel (PKG)

- Oversees six agencies; established in 1956.
- Members nine, cross party, appointed by Bundestag; support staff: nine.
- Chairman alternates every year between majority and opposition.
- Wide mandate: legislation, budget, administration and management, legality, effectiveness, surveillance, completed and ongoing operations.
- Powers: subpoena, access to information including operationally sensitive, visit sites, investigate complaints from officers and citizens. Two thirds can decide to start up an inquiry, with no need of a vote in plenary.
- Meets once a month; holds an annual public hearing with intelligence services directors.
- Deliberations are strictly confidential.
- MPs have access without security clearance, staffers are vetted.

102 Johnson, L.K., 2005. 'Governing in the Absence of Angels: On the Practice of Intelligence Accountability in the United States'. In: H. Born, L.K. Johnson, I. Leigh and A. Wills, eds. *Who's Watching the Spies? Establishing Intelligence Service Accountability*. Washington, D.C.: Potomac Books.

103 In most countries, parliamentary oversight reviews activities and programmes already implemented by intelligence services. One exception is the US Congress where a limited number of representatives are informed before sensitive intelligence programs are started. The *ex-ante* involvement of parliament does not necessarily allow them to participate in decision making or to stop operations, but may compromise their ability to criticise later if something goes wrong.

2.1.6. Expert intelligence oversight bodies

In addition to parliamentary committees, a growing number of countries have established expert intelligence oversight bodies that operate outside parliament. These bodies are typically composed of senior judges, civil society figures, and former politicians. Although appointed by and reporting to parliament and/or the executive, they are independent in structure and operation, often with their own budget, mandate, and full-time expert staff.

These non-parliamentary oversight bodies usually monitor the legality of intelligence operations and compliance with human rights, but may also assess effectiveness, administrative practices, or the use of intrusive methods. They often complement parliamentary committees, but some parliaments fully outsource intelligence oversight to such bodies.

This model addresses several weaknesses with parliamentary oversight:

- Operate full-time and continuously, unaffected by parliamentary recesses or elections.
- Offer institutional continuity through longer, fixed tenures.
- Are staffed by qualified professionals, selected for their expertise.
- Are generally seen as more independent, given their non-political status and restrictions on outside activities.

However, a key drawback can be their lack of direct democratic legitimacy. Since members are not elected, their accountability to the public may be less visible compared to parliamentary oversight.

Box 6. Examples of extra-parliamentary oversight bodies

Norway Parliament's Intelligence Oversight Committee (EOS)

- Oversees all Norwegian entities that engage in intelligence, surveillance and security activities, including the Defense Security Service.
- Established in 1996, by the Law on oversight of intelligence, surveillance and security service.
- Members: seven independent experts elected by parliament for a five-year term. A member can be reappointed once and be in place for a maximum of ten years. More than four members should not be replaced at the same time. Individuals who have previously worked in the services cannot be elected as committee members.
- Narrow mandate: oversight with focus on human rights protection and legality, receive complaints. Oversight of technical activities of the services, including the monitoring and gathering of information and the processing of personal data. No legislative power, no budget competency.
- Powers: Extensive right of access to information and premises (about 60 inspections a year. These are very well prepared inspections, with detailed instructions about what to inspect.
- Report to parliament (but first ask the service to solve problems and change practices).

German G 10 Commission

Eight senior experts review the use of extraordinary powers. Decides if surveillance measures are legal and necessary. Can refuse to approve operations.

2.1.7. Multistakeholder oversight of intelligence with law enforcement powers

The increasing complexity of intelligence oversight means that a single parliamentary committee, or, indeed, parliament alone, cannot ensure effective control. To address this, extra-parliamentary oversight bodies have evolved, growing in specialization and sophistication as states seek more professional, continuous, and legally robust mechanisms, especially for intelligence services with law enforcement powers.

This shift mirrors a broader European trend toward expert-led, rights-focused institutions that complement parliamentary scrutiny by adding legal rigor and operational expertise.

Austria offers an interesting example of complex, multi-stakeholder intelligence oversight through its integrated system of independent Legal Protection Officers (*Rechtsschutzbeauftragte*), created by an amendment to the Federal Constitution in 1997 as an independent organ for the protection of human rights in relation to the acts of the security police. The officer is not bound by any instructions.[104] The Austrian model stands out for combining intelligence and law enforcement oversight under a framework of legal specialization, institutional independence, and operational effectiveness.

- The institution of Legal Protection Officer is anchored in multiple legal statutes, including the Military Authorization Act, Criminal Procedure Code, Security Police Act, and the Financial Criminal Law. Together these establish a network of commissioners responsible for overseeing covert surveillance and intelligence activities across sectors. These include military intelligence, civilian security agencies, and financial crime enforcement.

- Each commissioner is a senior legal expert, appointed for a fixed term (typically five years), and operates independently of political influence.

- A key strength of this system lies in its legal rigor and real-time engagement. Legal Protection Officers must pre-authorize intrusive intelligence measures: for instance, communications interception, data collection, undercover operations, and license-plate surveillance. They must assess their legality and proportionality before they take place.

- They also have unrestricted access to security agency files, data, and premises, and are empowered to block or annul unlawful operations.

- Furthermore, they are obliged to inform individuals whose rights have been violated or to bring the case to Austria's Data Protection Authority.

- Their oversight is continuous, not reactive, and they submit annual reports to both the Interior Ministry and the Austrian parliament, reinforcing transparency and accountability.

This model effectively blends parliamentary and extra-parliamentary oversight, providing legal safeguards for individual rights while maintaining national security. It demonstrates how specialized, independent oversight bodies can complement parliamentary scrutiny and ensure robust, rights-based control over intelligence and surveillance activities.

104 European Union Agency for Fundamental Rights, 2016. *Austria Study: Data Surveillance II – Legal Update*, 30 June 2016. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/austria-study-data-surveillance-ii-legal-update-at.pdf [Accessed 17 October 2025]; See also European Court of Human Rights, *Ringler v. Austria*, Application No. 2309/10, Fifth Section, Decision of 12 May 2020. Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-203068%22]} [Accessed 17 October 2025].

The UK has a multi-layered system combining strong legal, technical, and parliamentary oversight of intelligence. The Investigatory Powers Commissioner's Office (IPCO) created under the 2016 Investigatory Powers Act,[105] oversees daily intelligence activities of agencies with investigatory powers. It functions as a powerful and well-resourced legal oversight body.

- There are fifteen judicial commissioners who approve interception warrants (known as a "double-lock" system).
- There are about 50 administrative and technical staff with legal and technological expertise.
- There is an ad-hoc Technology Advisory Board (TAB) of government, academic, and industry experts in ICT, convened as needed to address complex technical issues.

Oversight is further bolstered by the Investigatory Powers Tribunal, which hears complaints and can enforce redress, and the Intelligence and Security Committee (ISC) in Parliament, which has statutory inquiry powers.

A notable new trend in intelligence oversight in Europe is the creation of independent intelligence ombuds institutions, which complement the work of parliamentary committees and the judiciary by providing focused, expert, and rights-based scrutiny of intelligence activities. These bodies typically hold strong investigative powers, enjoy access to classified information, and have the ability to initiate legal or institutional action.

Finland's Intelligence Ombudsman,[106] established in 2019, represents a pioneering model of autonomous oversight, that works in tandem with the Parliamentary Intelligence Oversight Committee to form a comprehensive, multi-layered oversight system. Appointed by the Government for a five-year term, the Ombudsman supervises the legality of both civilian and military intelligence operations, monitors the use of secret surveillance methods, and ensures the protection of human rights.

- It has full unrestricted access to classified information and premises, the right to interview intelligence officials and other public employees as necessary.
- Can initiate inspections and investigations independently or in response to complaints.

105 Investigatory Powers Act 2016, c. 25, UK Public General Acts. Available at: https://www.legislation.gov.uk/ukpga/2016/25/contents [Accessed 17 October 2025].

106 Finnish Intelligence Oversight Authority, '*Duties and Powers*'. Available at: https://tiedusteluvalvonta.fi/en/duties-and-powers [Accessed 17 October 2025]. The institution also publishes an annual activity report.

- Has the authority to issue binding recommendations to intelligence agencies to correct or stop illegal practices, and can refer matters to court.
- Can refer cases directly to the courts, including the Intelligence Tribunal, if there are grounds to believe that an operation violates the law or human rights, and can submit opinions in court proceedings related to intelligence authorisations.
- Can propose that the Supreme Administrative Court annul or amend decisions of the Intelligence Tribunal or other oversight bodies if necessary.
- The office promotes best practices in intelligence gathering and evaluates the functionality of relevant legislation, offering proposals for legal reform.

Finland's Intelligence Ombudsman appears to be a leading benchmark in independent, legally empowered intelligence oversight, combining pre-approval powers, binding recommendations, court referrals, and full classified access. It is a uniquely powerful model.

Lithuania's Intelligence Ombudsperson[107] is appointed by the Seimas (parliament) and operates independently to strengthen the democratic oversight of intelligence services. The Ombudsperson investigates complaints from the public, assesses the legality of intelligence activities, and monitors the protection of individual rights in intelligence operations. This role adds an accessible, rights-focused oversight mechanism to Lithuania's accountability framework, reinforcing the rule of law in the intelligence domain.

Judicial control is an indispensable layer of intelligence oversight, ensuring that intrusive powers are used lawfully and proportionately. It includes both *ex-ante* authorization—where an independent court must approve intrusive measures such as surveillance before they are implemented—and *ex-post* review to assess their legality and impact after the fact. To be effective, legislation must clearly define the guiding principles for such measures, including legality, legitimacy, necessity, proportionality, subsidiarity, and ultima ratio. The judiciary also plays a broader role: it adjudicates cases of abuse or rights violations by intelligence agencies, offers remedies to individuals affected by unlawful interference, and ensures that intelligence laws comply with constitutional standards. In many democracies, judges or former judicial officials also contribute to parliamentary inquiries or oversight commissions, lending legal expertise to investigations. Where judicial approval is treated as a mere formality, oversight becomes hollow.

107 Republic of Lithuania, 2021. *Law on the Intelligence Ombudspersons*, No. XIV-868 (as last amended on 22 June 2023, No. XIV-2090). Available at https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f526bb834bee11ee8185e4f3ad07094a [Accessed 17 October 2025].

Box 7. What is the difference between parliamentary oversight and judicial authorization?

Parliamentary oversight focuses more on policies, while judicial oversight deals exclusively with narrow legal issues. The judiciary only reacts to legal matters brought before it. It cannot take initiatives on its own.

Parliamentary oversight is, in theory, unlimited. MPs have the democratic legitimacy to ask for information and explanation on any aspect of the work of a government agency, and they have the right to inspect premises and check intrusive capacities themselves.

Judges tend to demonstrate more deference to the executive branch on issues of national security and intelligence compared to MPs.

Although parliaments usually have little authority on operational affairs, they have extensive powers to determine the mandate and budget of security services, which gives them important leverage in influencing their conduct.

Investigative journalism remains one of the most powerful non-parliamentary tools for intelligence oversight. An independent media can uncover abuses or questionable practices that might otherwise remain hidden, prompting formal investigations and institutional reforms.108 Similarly, whistleblowers play a crucial role in bringing internal misconduct to light. Their willingness to speak out often comes at great personal risk, making it essential for parliaments to establish and enforce strong legal protections that shield them from retaliation.

All these developments highlight a growing commitment among democratic states to professionalize intelligence oversight through a multi-layered oversight system. This is one that extends beyond parliamentary mechanisms to include legally empowered, independent, and rights-based institutions capable of holding intelligence services to account.

108 A landmark example is the *New York Times*' 1974 *exposé* of Operation CHAOS—a covert CIA program targeting U.S. citizens. This led to the creation of the Church Committee, the most far-reaching inquiry into intelligence abuses in U.S. history. Johnson, L.K., 2015. A Season of Inquiry Revisited: The Church Committee Confronts America's Spy Agencies. Lawrence: University Press of Kansas.

2.1.8. Tools for parliamentary oversight

Although differing in organization, composition, mandate, and powers, intelligence oversight committees use similar tools. They are all founded on parliament's legal authority to obtain information from the executive. This includes demanding documents, reports, and summoning officials to explain and justify their actions.

Committees' oversight activities are independent from the plenary or from the legislative schedule. They set their own program and oversight agenda, decide whom to invite to hearings or meetings, which can be open or closed based on members' decisions. Effective oversight is a continuous process rather than isolated actions. Different tools suit different stages:

1. **Information gathering:** Reports, hearings, and field visits help committees understand the intelligence sector.

2. **Expertise development:** Oversight hearings and inquiries enable informed dialogue, clarifications, and independent analysis.

3. **Assessment and action:** With knowledge and expertise, committees can evaluate performance, identify weaknesses, and propose laws, amendments, or recommendations.

2.1.9. Reports

Reports are one of the most powerful and most frequently used oversight tools. Under the principles of the rule of law and separation of powers, all government departments, including intelligence services,[109] must report to parliament and the public,[110] ensuring democratic accountability. Reports allow parliament and other oversight bodies to verify compliance with government policy and the legal framework and assess whether taxpayers receive value for money.

109 Born, H. and Wills, A., 2012. *Overseeing Intelligence Services: A Toolkit. Geneva: DCAF*, 57. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/Born_Wills_Intelligence_oversight_TK_EN_0.pdf [Accessed 28 September 2025].

110 The UK is an exception as by law the main services, MI5 and MI6, produce an annual report for the Prime Minister and the Home Secretary. But they are not published for security reasons and no version is made available to the public. However, the independent oversight commissioners and the Intelligence and Security Committee publish their own reports on the work of the intelligence services.

There are two main types of reports:

1. **Regular activity reports:** Proactively submitted by intelligence and security services, usually annually,[111]regular activity reports are the most frequently used oversight instrument in parliamentary committees. These reports provide comprehensive information for oversight without compromising national security. Public versions may omit some sensitive details. Regular reports vary in length and detail depending on local practices and oversight mandates. Typically, they cover three areas: the agency's activities and task fulfilment, assessments of national and regional security threats, and oversight engagement including budgets.[112] Reports range from twenty pages (e.g. the Netherlands and Czechia) to over 160 pages (e.g. Australia's ASIO Annual Report, 2019-20).

2. **Special reports** are a supplement to the general yearly reports and are requested by the oversight body on specific topics identified to be problematic or of special interest. Often triggered by media scandals, security incidents, or targeted inquiries. Special reports require committees to ask precise, focused questions. The scope must be detailed enough to provide clear answers but limited enough to avoid being flooded with irrelevant information. Too much data can hinder effective oversight just as much as too little.

Box 8. What kind of special reports do intelligence oversight committees receive?

Based on legal requirements:

- The Slovene Parliamentary Control of Intelligence and Security Services Act (Art.19) provides that every four months and, more often, if necessary, the service reports to the parliamentary Committee on the application of intrusive measures (for both national security and criminal investigations). Reports include the number of cases in which measures have been ordered, the number of persons against whom measures have been ordered and applied, the number of rejected proposals, the legal grounds for ordering measures in individual cases, the number and type of communication means intercepted in individual cases, the time period for which individual measures have been ordered, data

111 Sometimes more frequently. For example in Slovenia or the US on a quarterly basis.

112 See, for example, links to recent public reports of the main intelligence services from Australia, Canada, Croatia, Czechia and the Netherlands at, respectively, the following links: ASIO Annual Report 2019-20: https://www.asio.gov.au/asio-report-parliament.html [Accessed 17 October 2025]; CSIS Public Report 2019: https://www.canada.ca/en/security-intelligence-service/corporate/publications/2019-public-report.html [Accessed 17 October 2025]; Security-Intelligence Agency 2019: https://www.soa.hr/hr/dokumenti/javni-dokumenti-soa-e/ [Accessed 17 October 2025]; Security Information Service 2018 https://www.bis.cz/annual-reports/ [Accessed 17 October 2025]; AIVD Annual Report 2019: https://english.aivd.nl/publications/annual-report/2020/09/03/aivd-annual-report-2019 [Accessed 17 October 2025].

on established irregularities in applying the measures in individual cases. Reports also contain data on measures that have not yet been concluded. The Committee may request a detailed report on particular measures.

- Section 195 of the Criminal Code of Canada requires as a measure of accountability the Minister of Public Safety and Emergency Preparedness to report to Parliament on the use of electronic surveillance in the investigation of offences that are under the remit of the Attorney General.

Based on focused inquiries:

- The UK Intelligence and Security Committee of Parliament (ISC, in charge of oversight of all UK Intelligence Agencies) initiates such reports autonomously if deemed appropriate. An example is the 2017 Special Report on UK Lethal Drone Strikes in Syria, which was conducted to assess the intelligence basis for lethal drone strikes on UK citizens. The ISC held oral evidence sessions and received written material and original intelligence reports from intelligence agencies. On that basis the report was produced and reported on, as in most cases, to the Prime Minister and to Parliament (with sensitive material redacted).[113]

For report-based oversight to be effective, a parliament must set clear and strict deadlines for report submission and their review in committee or plenary.

Reports from government departments—especially intelligence agencies—often serve public relations purposes and may not present the full picture. However, they are a valuable starting point for oversight, helping committees identify key questions and guide further investigation using more in-depth tools.

2.1.10. Hearings

Hearings, if properly used, can be one of parliament's most effective oversight tools. The hearing agenda often reflects the key political and security issues of the day. Under its constitutional right to seek information from the executive, a parliament (through its committees) may summon executive officials as often as needed to supplement regular reporting.

113 Intelligence and Security Committee of Parliament (ISC), 2017. UK Lethal Drone Strikes in Syria. HC 1152. Presented to Parliament by the Intelligence and Security Committee of Parliament on 26 April 2017. Available at: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20170426_UK_Lethal_Drone_Strikes_in_Syria_Report.pdf [Accessed 5 November 2025], 1 – 4.

Some parliaments distinguish between consultative and oversight hearings:

Consultative Hearings are held primarily for legislative or policy discussions. These hearings bring together government officials, experts, and other stakeholders to inform the legislative process. They help committees:

- Review existing laws
- Evaluate draft legislation
- Understand emerging issues

The detailed, first-hand information obtained during the hearing should enable the committee to make better informed analyses and decisions. These hearings are often public, improving transparency. However, some are informal, with no verbatim record.

Oversight hearings focus on accountability, and seek in-depth information or evidence on specific matters, including misconduct, abuse of power, or policy failures. Government officials—sometimes under legal obligation—attend and may be asked to submit documents in advance. Experts from civil society, academia, or other independent institutions may also be invited.

- Oversight hearings are often held *in camera*, to encourage senior agency employees to share information.

- If the topic of the hearing is very sensitive for national security, there is limited or no communication with the press and the public about the content of discussions or even about the occurrence of the event.

- Written and oral evidence taken at the hearings is included in the record of the committee. In some parliaments, evidence can be taken only following a decision of the plenary, and in others permanent committees are empowered to take evidence during a parliamentary inquiry.

However, most parliaments do not make such distinctions formal, as most hearings appear to blend lawmaking, oversight, and impeachment purposes. The effectiveness of hearings as an oversight tool depends on several factors.

Committee independence

- Committees typically decide independently when to hold hearings and whom to invite.

- A simple majority vote usually suffices to set the agenda, determine attendees, and decide if the hearing is public or closed.

Investigative powers

- Some committees can summon only government officials; others may invite a broad range of actors including experts, NGO representatives, civil society, academics,
and citizens.
- Diverse input helps counterbalance the executive's control over security-related information.
- Effective hearings require thorough preparation, coordinated questioning, and broad topic coverage.

Follow-up capacity

- Committees must ensure hearings lead to actionable outcomes: reports, recommendations, or even the establishment of inquiry committees.
- If evidence is insufficient or indicates deeper issues, the committee may, in most parliaments, request a formal inquiry with subpoena powers.
- Public hearings increase transparency and public trust, and can generate political pressure for implementation.

Box 9. Hearings in German Intelligence Oversight Committee

The parliamentary intelligence oversight committee of the German Parliament (PKGr), has started organising **yearly public hearings** of the directors of the three intelligence services under its supervision, including the director of military intelligence (MAD). The directors inform the committee about mains trends and incidents of importance in their area of activity.[114]

A series of focused hearings conducted by the committee since 2017 on the influence and propagation of the far right in the German armed forces led in September 2020 to the dismissal of the director of MAD by the Minister of Defence. The elite KSK (Special Forces Command) was also partially disbanded in June 2020, as twenty of its members were suspected of right-wing extremism.

114 Deutscher Bundestag, 2020. "*Parlamentarisches Kontrollgremium (PKGr)"*, Available at: https://www.bundestag.de/dokumente/textarchiv/2020/kw27-pa-parlamentarisches-kontrollgremium-bnd-699648 [Accessed 17 October 2025].

2.1.11. Field visits

Field visits are powerful oversight tools as they give members of parliament direct access to intelligence operations and personnel. Unlike hearings held in parliament buildings, field visits allow MPs to engage with a broader range of military and civilian staff. They can inspect facilities, review equipment and documentation, and gain first-hand insight into operational realities. For intelligence and security institutions, these visits offer an opportunity to explain operational challenges, build trust with the oversight body, and advocate for legislative or budgetary support.

Unlike hearings, which are based on interaction and dialogue with officials who come to the committee, on a field visit the committee goes out in an explorative mission. The risk of losing focus and of getting derailed from its oversight objective is high. Therefore, the need for relying on expert staff support is more relevant in field visits than in other oversight activities.

Clear procedures are another prerequisite for successful field visits. The Committee Rules of Procedure should clearly detail responsibilities and steps in implementing a field visit in order to allow for efficient and smooth decision making in all its stages. Field visits can be monitored following three main phases: preparation, implementation and post-visit follow up. The nature of these phases will depend on whether the visit is organised as a proactive oversight activity (announced well in advance, eventually included in the annual programme of the committee), or, whether it is a reactive visit to carry out an investigation of some specific allegation or incident. In intelligence oversight, even inspection visits labelled as "un-announced" are usually communicated 24-48 hours in advance.

Box 10. How to develop a committee's experience in organising field visits?

- Ideally the committee rules of procedure will describe with clarity how field visits are organised. If not in the rules of procedure, an overall protocol should be agreed on at the outset of committee's mandate that includes both planned and unannounced visits.
- A new committee should start with visits announced in advance, on general topics and objectives, such as a better understanding of the intelligence organisation, its functions and activities. A study visit at the headquarters building is the best starting point to get an overview of the operations, the administration etc., before moving on to more specific functional/ regional offices.

- This gives both the committees and the services the opportunity to learn about each other's perspectives and get acquainted to visits in a non-conflictual way.
- It may be useful to plan for a period of announced visits and to agree on a starting point from which unannounced visits can begin. Even in an "announced visit period", visits should be able to take place on short notice in urgent situations.
- When committee members have security clearances, check that these, as well as the clearance of the accompanying staff are at the needed level (depending with the objective and topic of the field visit) and that they cover physical access to the sites and facilities.
- Ensure the services understand the "need to know" principle for the specific oversight mandate of the committee, including the legal authority of the committee and the legal foundation for the committee oversight mandate.
- Leave the most sensitive sites (like interception facilities) for a later stage, when the committee has acquired a good understanding of the overall picture, so that they know better *what* and *how* to ask.
- A good preparastion is crucial for the success of the visit; a lack of good understanding of the legislation and the functioning of the services might give a poor impression of the committee. It is also a missed opportunity for establishing and improving oversight.

2.1.12. Inquiries

Inquiries are a very strong instrument of oversight and are able to reveal facts hidden by the government. They are not only an oversight instrument but an effective way to better understand an issue and develop improved policy or legislation. Inquiries are always conducted in the framework of a specific and narrow mandate. The topic, the scope and the timeline of the inquiry are all carefully defined.

A parliamentary inquiry requires special powers of investigation, also called subpoena powers. This means that the rules of criminal procedure shall apply *mutatis mutandis* in the taking of evidence. Inquiry committees are provided with the same powers as investigative judges: they can summon witnesses, demand documents and other items, and often they employ legal means to enforce their demands. What distinguishes inquiries from other forms of parliamentary investigation is that their powers extend not only to members of government and public officials. They also extend to members of the public. In most European countries, inquiry committees can summon any official or private citizen

without exceptions or limitations (this is a major difference from hearings). The summoned citizens must appear, provide explanations, reply to questions, and provide documents and information to the committee under oath, much as with a testimony in a court of law and with the same consequences for failure to provide the truth. However, these investigative powers can be employed only in relation to the immediate matter of inquiry and their duration is limited in time, by the mandate of inquiry.

Parliamentary rules of procedure will provide clear instructions about the conditions in which an inquiry are initiated, allowing equitable participation of opposition and minority groups in decisions about the organisation and the mandate of an inquiry. Very few standing committees have the power to lead inquiries and when they do, they must obtain a mandate and a permission from the plenary (exceptions are Belgium, Canada, Germany, Montenegro and the Netherlands).

Most often, parliamentary inquiries are led by ad-hoc cross-party inquiry committees. They are set up by a decision/resolution of the parliament in its plenary, with the mandate to collect information on particular incidents or episodes of pressing political concern. The inquiry committees are initiated after the event, but within a reasonable timeframe so that lessons can be learned promptly. They are given a deadline to conduct their investigations. After submitting their final report to parliament, the committee is dissolved.

Despite the similarities between their proceedings and those of judicial procedures, inquiry committees should not be confused with criminal investigations. They do not assess or assign criminal responsibility. Inquiry reports are of a political nature. Their conclusions or resolutions are not legally binding on their own. For these reasons, inquiries should be deployed with care.

Box 11. What special investigation powers do inquiry committees have?

In the German Bundestag the Defence Committee has an outstanding position because its settling is provided for in the constitution and it is the only committee which can declare itself a committee of inquiry (Art. 45a, para (2) of the Basic Law). In the case of all other committees, parliament must take a decision to this effect. A committee of inquiry is the German parliament's most effective weapon for scrutinizing the government's conduct, having similar rights to the Public Prosecution Office.

- Meetings in which evidence is taken are open to the public, unless military secrecy is required. Meetings at which the evidence is evaluated are not open to the public.

- An administrative fine of up to €10,000 can be placed on absent witnesses or on those who refuse to surrender an item required by the inquiry committee as evidence.[115] In instances of a repeated failure to comply, the administrative penalty may be levied again.

- A witness who refuses to testify can be obliged to attend by the investigative judge at the Federal Court of Justice, upon receipt of an application from the inquiry committee supported by one quarter of its members. The witness may be held in custody in order to compel them to testify.[116] The judge can also order the seizure of items in a search if requested by the inquiry committee as they amass evidence.[117]

- The federal government is required to grant the necessary authorization for the examination of office holders.[118]

- In France, the refusal to appear in front of an inquiry committee and to respond to its questions can be punishable by up to two years of imprisonment and a fine of €7,500 [119].

US Congress Committees possess subpoena powers; refusal to testify before a committee or failure to provide a requested document is considered Contempt of Congress, and it is punishable with up to one year of prison and a $1,000 fine.

Montenegro's Law on Parliamentary Oversight in the Area of Security and Defence provides penalties for failure to respond to committee summons or to provide the required information (Art.22), prescribing fines that can go up to €2,000 for employees and €20.000 for legal entities.

115 Gesetz zur Regelung des Rechts der Untersuchungsausschüsse des Deutschen Bundestages (PUAG) [Law on Inquiry Committees], §§ 21, 27, 29, BGBl. I 2001 S. 1142. Available at: https://www.gesetze-im-internet.de/puag/BJNR114210001.html. [Accessed 5 November 2025]

116 Ibid. Section 27 (2).

117 Ibid. Section 29 (3).

118 Section 23 of the Law on Inquiry Committees. See also Section 54 (4) of the CPC of Germany on the examination of public officials who are no longer in service. Available at: https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html [Accessed 17 October 2025]. Further analysis of special legislation would be needed to clarify whether former civil servants are obliged to testify, but it seems that they are.

119 Ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires, art. 6, JORF 17 Nov. 1958. Available at: https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000035391366. [Accessed 5 November 2025]

In practice, inquiries remain a rarely used oversight tool, typically reserved for exceptional circumstances[120] involving significant concerns. While their use should be limited and carefully justified to avoid politicization or the perception of a "witch hunt", when inquiries are conducted fairly, transparently, and with a clear mandate, they can produce transformative results. Here are a few examples of parliamentary inquiries into intelligence, defence, or security sector conduct.

In the United States, several landmark congressional inquiries uncovered serious abuses, triggered major legislative reforms and marked profound shifts in public and institutional attitudes toward intelligence accountability. **The Church Committee**[121] was created in response to explosive revelations around the U.S. Army's program of domestic surveillance and an article published in the New York Times in December 1974, exposing assassination attempts on foreign officials by the CIA. The Church Committee conducted a yearlong investigation into American intelligence agencies including 126 full committee meetings, 40 subcommittee hearings, with 800 witnesses interviewed in public and closed sessions, and 110,000 documents analysed. The final report published in April 1976 included 96 recommendations designed to redefine the relationship between intelligence and democracy leading to the creation of legal and institutional safeguards that firmly placed intelligence activity under permanent congressional oversight, judicial review and legal constraints. The Iran-Contra Congressional Committee[122] exposed in 1987 that parts of President Reagan's administration had secretly carried out actions that were not authorized by Congress or in line with U.S. law. Specifically, the administration sold weapons to Iran—a country under an arms embargo at the time—and used the money from those sales to secretly support a rebel group in Nicaragua called the Contras. This was done despite a congressional ban on funding the Contras, making the operation illegal and a major violation of democratic oversight. The inquiry underscored the need for more robust, institutionalized oversight mechanisms, and it reaffirmed the constitutional principle that intelligence activities must remain accountable to democratic institutions.

In Germany, the NSA Inquiry[123] was launched in the Bundestag in March 2014, to investigate the extent of foreign secret services spying in Germany. The committee met 131 times over a period of three years; 66 times in public meetings. High level public officials, including Chancellor Angela Merkel, have been heard. Initially triggered by Edward Snowden's revelations, the inquiry transformed to investigate the legality of German intelligence governance and

120 Most parliaments create inquiry committees only a few times during a legislative term. For example, the House of Representatives in the Netherlands has created only ten inquiry committees in the last three decades.

121 Information about the inquiry committee and its Report available at: https://www.senate.gov/about/powers-procedures/investigations/church-committee.htm [Accessed 17 October 2025].

122 Also called the *Inouye-Hamilton Committee*. The "Report of the Congressional Committees Investigating the Iran-Contra Affair" is available at: https://archive.org/details/reportofcongress0000dani [Accessed 17 October 2025].

123 Chase, J., 2017. '*NSA spying scandal: Committee presents controversial final report*', *Deutsche Welle*, 28 June. Available at: https://www.dw.com/en/nsa-spying-scandal-committee-presents-controversial-final-report/a-39453668 [Accessed 17 October 2025].

has identified important oversight deficits, opening the way to major intelligence reforms. In 2016, WikiLeaks released over 2,400 documents which it claims are from the investigation.

Following the devastating terrorist attacks on Charlie Hebdo and the Bataclan in 2015, the French Parliament established an Inquiry Committee to examine the state's counter-terrorism response. The investigation spanned over six months and involved 59 hearings and nearly 190 interviews. The resulting three hundred-page report revealed significant shortcomings in the coordination and effectiveness of France's intelligence services, particularly in monitoring known radicalized individuals and addressing radicalization within prisons. The Committee issued 40 concrete recommendations aimed at improving intelligence sharing, reinforcing prison intelligence, and strengthening the legal framework for counter-terrorism.

In 2006, the Romanian Senate established an *ad-hoc* inquiry committee that, over two years, investigated the existence of CIA secret detention sites on national territory. The report was kept entirely secret except for its conclusions, which categorically deny the possibility that secret detention facilities could be hosted on Romanian soil. However, these conclusions were contradicted by the Fava Inquiry of the European Parliament (2007) and by the ECHR case *Al Nashiri v. Romania* (2018).

In 1994, the Dutch parliament created a parliamentary commission of inquiry into criminal investigation methods used in the Netherlands and the control exercised over such methods. The committee conducted preliminary interviews with over 300 persons, followed by "confidential conversations" with 139 persons, and 93 public hearings directly broadcasted on national television. The 6,700-page report, published in 1996, had a significant impact on the organisation of criminal investigations in the Netherlands, leading to major legislative reforms.

The UK's Intelligence and Security Committee conducted, in Parliament, an inquiry, over the course of eight months, into the threat posed by Russia to the UK (cyber, disinformation, and influence) and looked also at the response of the UK government. The report was published in July 2020.[124]

These examples show that well-structured and principled inquiries can be powerful tools for renewing democratic control and improving the governance of intelligence services. Far from weakening intelligence agencies or compromising their operational effectiveness., parliamentary inquiries can lead to meaningful institutional reforms, reinforce services legitimacy and enhance public trust.

124 Intelligence and Security Committee of Parliament, Russia (HC 632), Presented to Parliament pursuant to section 3 of the Justice and Security Act 2013, 21 July 2020. Available at: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20200721_HC632_CCS001_CCS1019402408-001_ISC_Russia_Report_Web_Accessible.pdf. [Accessed 5 November 2025]

Inquiries receive more public attention than regular parliamentary activities. Their urgency and visibility activate all committee members, who shift from routine oversight to crisis response. Well-conducted inquiries demonstrate the capacity of parliaments to confront serious issues. By bringing visibility, relevance, and a sense of purpose, they enhance the credibility and legitimacy of a parliament within the democratic system.

2.1.13. Strategies for strengthening parliamentary oversight

Effective oversight requires a clear legal mandate, consistent political commitment, and regular implementation. Here are some strategies that can help committees to make full use of their legal authority and to engage in effective intelligence oversight.

Clarify the regulatory base of intelligence

Effective oversight of intelligence must start with a very clear inventory of each service and its functions, missions and powers. Those must be correlated with the existent national legislation, and eventual gaps must be addressed in a legislative development plan.

- The law must be clear, foreseeable and accessible. It must describe clearly the mission, organization, powers, and restrictions in the use of special powers.
- Safeguards against arbitrary action must counterbalance secrecy and guarantee against discretionary power and lack of accountability.
- Ministerial orders, internal procedures and rules of conduct should be requested and consulted by oversight bodies, to ensure they comply with existing public laws and the constitution.
- Regulations that are not made public should cover only specific information that could jeopardise intelligence work and/or national security if made public (such as operational methods and the use of particular devices or technologies).

Improve committees' access to information

Access to information is a core challenge for intelligence oversight. The need for secrecy is constantly used to shield agencies from democratic scrutiny.

Parliamentary intelligence committees access classified information under one of two models:

1. **Without security clearance** – This is common in Europe where MPs access classified data based on their mandate, with a secrecy oath and legal liability for leaks.

2. **With security clearance** – This is used in some countries (e.g., Estonia, Hungary, Latvia, Lithuania, North Macedonia, Serbia,). MPs undergo vetting by intelligence services. While this can build trust, it risks undermining parliamentary independence if not carefully designed.

Several risks are associated with granting access through security clearances:

- **Conflict of interest:** Oversight bodies are sometimes vetted by the very agencies they supervise. To mitigate this, the agency should provide only an advisory opinion, while the final decision should rest with a given parliament. There must also be a right to appeal denied clearances.

- **Unequal access within committees:** If some MPs are denied clearance, it can undermine committee cohesion and credibility. To avoid this, clearance procedures should be completed before committee appointments.

- **Disclosure risks:** Even with clearance, MPs may unintentionally leak classified information. However, continued dialogue with intelligence agencies can foster a culture of responsibility. In most countries, MPs are not immune from prosecution for unauthorized disclosures.

With or without a security clearance, parliamentarians must understand that full access to all classified information is neither necessary nor feasible. First, a committee's right to information must be directly linked to its legal **mandate**, which must be very well defined in law and rules of procedure. If a parliament fails to do this, the executive gains discretion to decide what information to share—weakening oversight. Second, even with formal authorization, information should only be shared when necessary for fulfilling official duties. The **need-to-know principle** should prevent misuse or indiscriminate browsing of sensitive data.

Laws should specify exceptions to access rather than define what may be shared. This ensures that all non-exempt information is available by default. The categories of information that usually constitute such exceptions are the following:

1. **Ongoing operations:** Disclosing active operations may compromise outcomes or endanger personnel. However, some operations are long-running, and the definition of "ongoing" is often left to the agency's discretion, which can be misused.

2. **Sources and methods:** Protecting the identity of human sources and intelligence-gathering techniques is essential. However, if oversight relates to serious criminal allegations or human rights violations, limited access may be necessary.

3. **Foreign-origin information:** Shared through international cooperation, such information is protected under the "third party rule," requiring the originating country's permission for disclosure. Yet, this practice can significantly restrict oversight, especially as foreign intelligence sharing has become a major component of modern intelligence work. Oversight bodies across Europe are increasingly seeking exemptions or improved access in this area.

4. **Judicial or criminal investigations:** Oversight must not interfere with ongoing investigations or judicial proceedings. Temporary limits are justified to preserve the right to a fair trial and investigative integrity, but access should resume after these processes conclude.

Box 12. What kind of information is exempt from access in different national laws?

- Ongoing or future intelligence operations, information that might reveal the identity of undercover officers, sources methods and means. The exception from access does not apply in situations where a court established infringements of human rights and liberties (Romania).
- Documents of foreign services or documents that would affect the personal rights of third parties (Germany).
- Ongoing judicial proceedings or criminal investigations (most countries).
- Information that might jeopardize national interests or the safety of persons (Austria).
- Information that might jeopardize the security of the Republic (Italy).
- Sensitive information (UK).
- Operationally sensitive information (France).
- Information that could reveal the identity of a source or that would impair the rights of third parties (Luxembourg).

Access to information has its perils. Classified information can be used by the services to mislead or influence politicians by showing them selective information. Classified information can also be used as an efficient instrument to reduce parliament to silence, as once they receive classified information about a topic they cannot discuss the matter in public.

Parliamentary committees must strive to obtain information that matches their oversight responsibilities. That means they need to go beyond following the "paper trail" and the comparison of statistical data made available by different agencies. They need to develop sufficient fact-finding abilities to effectively investigate conduct and records in the possession of intelligence agencies.

Box 13. How can access to information be improved?

- Adopt clear rules and procedures for access, debate, storage and dissemination of classified information, including internal committee rules on what can be communicated (1) within the parliament; (2) to the public.
- Adopt clear procedures for gaining and maintaining security clearance, for both parliamentarians and committee staff.
- Dedicate special premises and facilities for handling/reading/discussing sensitive information (such as a shielded room for in camera committee meetings, not accessible to the public, nor to parliamentarians who are not members of the oversight committee).
- Employ qualified staff responsible for handling classified documents (and ensure their frequent training).
- Organise *in camera* meetings on sensitive topics.
- Link any request for information to the oversight mandate of the committee (make precise reference to articles in constitution, laws, rules of procedure).
- Prevent over classification through laws that define clearly and restrictively the types of information that can be classified, and through an independent agency for the oversight of the classification system
- Introduce a requirement for intelligence agencies and governments to proactively disclose certain types of information to the committee, without waiting to be requested to do so.

Improve committee expertise

The biggest problem in oversight is the asymmetry of information and expertise that exists between parliament and the intelligence services. Parliamentarians with deep knowledge of security and intelligence are rare, while intelligence agencies hold the advantage in expertise, information access, and control over their operations. Effective oversight depends heavily on the executive and intelligence services being willing to share information and guide MPs.

Developing expertise is essential for meaningful oversight. Committee members and staff need a strong grasp of the law, policy, and intelligence functions to assess whether agencies comply with democracy, human rights, and legal standards. Key areas of expertise include:

1. **Democratic oversight expertise:** Understanding parliament's role in democracy, oversight tools, and procedures. MPs must grasp the principles of democratic accountability and develop the political will to engage in oversight.

2. **Legal expertise:** Knowledge of the legal framework governing intelligence, including mandates, human rights limits, use of special powers (e.g., recruitment, surveillance), data protection, and complaint mechanisms for citizens and staff.

3. **Operational expertise:** Insight into how intelligence services function across civil, military, and law enforcement domains; intelligence collection methods (HUMINT, COMINT, OSINT, IMINT, cyber operations); international cooperation; and agency roles and priorities.

4. **Technological expertise:** Understanding evolving ICT and data management technologies, which underpin modern intelligence work. MPs must grasp technological realities to make sound legal and policy assessments, especially in the digital age with big data and AI-driven capabilities.

Gaining expertise in intelligence oversight is a slow process requiring dedication, typically taking eighteen to twenty-four months and depending heavily on the cooperation of the intelligence services. Given the frequent turnover of committee members after elections, building strong, professional parliamentary staff is essential. Without such staff, MPs rely primarily on information provided by the very agencies they are meant to oversee, limiting the depth and independence of scrutiny.

Committee staff play vital roles. They organize meetings, liaise with government, collect and interpret information, provide legal advice, draft legislation and reports, and plan oversight activities. In most parliaments, staff members are vetted to access classified information, which ensures security but also enables them to support the committee's work with both expertise and access. Stable, skilled staff ensure continuity, institutional memory, and the committee's ability to fulfil its duties effectively.

Clarify committee procedures

Parliamentary procedures (or "Standing Orders") are rules and customs that govern parliamentary meetings and activities. Adopted at the start of each legislative term, they ensure smooth functioning and uphold members' rights, balancing majority rule with minority protections.

Most parliamentary committees have their mandate and powers defined broadly by law and general rules of procedures, granting legal authority to act. However, sensitive committees like those overseeing intelligence often have detailed mandates set by special parliamentary decisions, reinforcing their legitimacy and parliamentary support. Intelligence Oversight Committees adopt their own rules of procedure at the start of their term to clarify mandates and to streamline decision-making. These typically cover:

- The scope of the committee's competency updated as needed to reflect institutional changes or evolving oversight needs.
- Roles and responsibilities of the chair, deputies, and staff.
- Procedures for convening meetings and quorum requirements to prevent deadlocks.
- Debate and voting rules that protect minority participation.
- Provisions for member representation during absences.

Organize joint meetings and oversight activities

Effective intelligence oversight requires multiple parliamentary—and sometimes non-parliamentary—bodies with overlapping but complementary mandates. However, gaps between these mandates can allow intelligence services to evade scrutiny. Therefore, communication, expert collaboration, and joint action among committees are essential for ensuring meaningful oversight.

1. **Comprehensive Understanding:** Intelligence is complex and interconnected. Oversight must reflect the integrated nature of today's transnational threats, cross-agency cooperation, and blurred public-private roles. Functional oversight demands a holistic view of the entire intelligence ecosystem, not only isolated agency reviews.

2. **Pooling Resources and Expertise:** Oversight resources are limited compared to those of intelligence services. Sharing expertise and experience across committees helps address information asymmetry and strengthens overall oversight capacity.

3. **Enhanced Political Influence:** Committees lack enforcement power and rely on persuasion and publicity. United, multi-committee action increases legitimacy, political weight, and influence over the executive and intelligence agencies.

For these reasons, cooperation between defence, security, law enforcement, and intelligence committees is vital. Committees should define when and how to collaborate:

- **Informally:** *Ad-hoc* joint debates, hearings, investigations, or field visits on shared issues.
- **Formally:** Including joint meeting procedures in their rules of procedure to institutionalize collaboration.
- **On a case-by-case basis:** Sitting together with other relevant committees to discuss policy, legislation, or oversight activities.

The focus should be on effective, results-driven oversight rather than the number or type of bodies involved.

2.1.14. Conclusion

In most democratic systems, the constitutional framework and existing legislation already provide a legal basis and institutional tools for meaningful intelligence oversight. What matters most is whether parliamentarians choose to use the powers they have. Effective oversight does not require vast resources or ideal conditions. A few committed members equipped with the determination to ask the right questions and the courage to expose irregularities, can trigger real accountability. Even a single vigilant legislator can make a significant difference by engaging peers, mobilizing committees, and keeping intelligence agencies within legal and ethical boundaries. Persistence and integrity can foster a culture of oversight that holds even the most secretive parts of the state to account. In the end, democratic control of intelligence is less a matter of legal possibility than of political choice.

2.2. Assessing and overseeing intelligence and law enforcement in the Euro-Atlantic area

Andrej Bozhinovski

2.2.1. Introduction

The modern world is facing evolving threats, from terrorism and organized crime to cyberattacks and interference by foreign powers. These threats have led to growing intersections between intelligence and law enforcement functions. The present research provides a perspective on how intelligence services are regulated, highlighting the evolution of their roles, the shifting boundaries between intelligence and law enforcement, and the mechanisms developed to ensure oversight and accountability. The aim is to offer both a doctrinal and practical perspective on how the judicial oversight of intelligence is implemented and where it can be improved. This research employs normative and comparative methods for qualitative analysis of legal sources, case law, and court rulings from the European Court of Human Rights (ECtHR), the EU Court of Justice (CJEU) and court decisions. These bodies provide authoritative perspectives on oversight principles and requirements. The first part of the research examines the definition and development of intelligence services with law enforcement mandates. The second part explores different oversight mechanisms, including parliamentary, executive, and judicial oversight, as well as the role of the media and whistleblowers in ensuring accountability. The study concludes with policy recommendations tailored for the emerging challenges of the AI era.

2.2.2. Defining intelligence service with law enforcement mandates: Evolution, boundaries and overlaps

Global security challenges such as the fight against terrorism, cybersecurity threats, the proliferation of weapons of mass destruction, organized crime, corruption, and drug trafficking, have fundamentally reshaped the aims, character, and tools of criminal law. In response, states have adopted measures grounded in the rule of law that permit investigators and prosecutors to use intelligence and sensitive law enforcement information as evidence in court to prosecute terror

and organized crimes.[125] These measures are designed to safeguard both the confidentiality of sources and investigative methods, as well as the defendant's right to a fair trial as a core procedural guarantee. In most European Union (EU) countries, however, evidence obtained by intelligence services (referred to here as 'intelligence-gathered evidence') is generally admitted in judicial proceedings only as background information.

The distinction between intelligence services and law enforcement from legal and institutional perspective has grown increasingly. Indeed, today, the central debate no longer centres on institutional separation, but on the functional limits and the oversight mechanisms that ensure the democratic legitimacy of the work of intelligence services equipped with law-enforcement powers. Different sources define intelligence services in different ways. DCAF defines them as *specialized state agencies*, whose structural mandate may be delineated, integrated, or hybrid, depending on whether they are legally empowered to perform criminal investigations, effect arrests, or gather admissible evidence.[126] In addition to this, the policing community has adopted intelligence not only as a source of information but also as a methodology and decision-making process, something outlined in the *OSCE Guidebook on Intelligence-Led Policing.* Intelligence here could be defined as a "methodology, structure, process, and product," designed to transform raw data into actionable law enforcement strategy. From a regulatory perspective, this convergence is already reflected in key international documents.[127] Furthermore, The OECD's 2022 Declaration on access to data held by private-sector actors treats national-security and criminal-justice demands within a unified governance framework, requiring both sectors to adhere to the common standards of legality, transparency, and oversight.[128] Evidently this definition evolves over time, and a practical takeaway is that a given body becomes an intelligence service with law-enforcement powers when it both produces security intelligence and is legally authorized to exercise some dimension of criminal-procedural authority. This might be internally (hybrid) or *via* collaboration with police structures (integrated).

Nonetheless, the necessity of clear legal boundaries is evident in order to protect the democratic accountability of these services. In Europe, the Parliamentary Assembly of the Council of Europe's Recommendation 1402

125 Bozhinovski, A., 2021. Admissibility of (Counter) Intelligence Evidence Information in Court-Thematic Brief. *DCAF Geneva Center for Security Sector Governance.* Available at: https://www.dcaf.ch/admissibility-counter-intelligence-information-evidence-court [Accessed 4 October 2025].

126 DCAF, 2020. *Counterintelligence and Law Enforcement Functions in the Intelligence Sector*. Geneva: Geneva Centre for Security Sector Governance. Available at: https://www.dcaf.ch/counterintelligence-and-law-enforcement-functions-intelligence-sector [Accessed 4 October 2025], 5.

127 Organisation for Economic Co-operation and Development (OECD), 2017. Guidebook on Intelligence-Led Policing. Vienna. Available at: https://policehumanrightsresources.org/content/uploads/2018/05/OSCE-Guidebook-Intelligence-Led-Policing.pdf?x54919. [Accessed 5 November 2025].

128 Organisation for Economic Co-operation and Development (OECD), 2022. *Declaration on Government Access to Personal Data Held by Private Sector Entities*. OECD Legal Instruments, OECD/LEGAL/0487. Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487 [Accessed 4 October 2025], 7-9.

emphasizes that internal intelligence services must not be allowed to arrest or detain individuals except in narrowly defined circumstances vital to national security interests.[129] Likewise, the Venice Commission, in its report on Signal Intelligence Agencies (SIGINT), emphasized that oversight mechanisms must apply the principle of proportionality in accordance with the degree of intrusiveness of the surveillance. This is especially so as bulk data collection increasingly includes domestic communications.[130] Concerning the protection of the gathered data, EU Directive 2016/680 establishes core principles mirroring the requirements form the jurisprudence of the CJEU and the ECtHR such as the existence of a legitimate purpose, limitation, necessity, and proportionality into criminal-justice data processing. This effectively replaces the former national-security exception under EU law.[131]

2.2.2.1. The evolution

The *Pre-9/11 Era* saw the functional separation of police and intelligence agencies, with strong judicial oversight and reactive approaches to security. The post-9/11 Era (2001–circa 2016/2018) began with the September 11 attacks, which triggered a paradigm shift toward integration, proactive intelligence, and fusion centres to better prevent terrorism and organized crime. The Digital Era (from around 2016/2018 onward) emerged as digital technology, big data, and cybercrime transformed law enforcement, leading to rapid, automated cross-border information exchange and new legal frameworks such as EU Directive 2023/977. The dividing lines correspond to the global impact of 9/11 and the subsequent digital transformation of security practices.[132] Building on this, the regulation of intelligence and law enforcement cooperation has evolved through three distinct periods:

1. *Pre 9/11 Era.* In the 1990s, most European states created internal civilian security agencies formally separated from the police, emphasizing functional segmentation and judicial control. This period saw functional segmentation and reinforced judicial oversight over intelligence operations.

129 Parliamentary Assembly of the Council of Europe, 1999. *Recommendation 1402 (1999) on Control of Internal Security Services in Council of Europe Member States. Strasbourg: Council of Europe*. Available at: https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16689&lang=en [Accessed 4 October 2025], para 6.

130 European Commission for Democracy through Law (Venice Commission), 2015. *Report on the Democratic Oversight of Signals Intelligence Agencies*. CDL-AD(2015)011. Strasbourg: Council of Europe. Available at: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=cdl-ad%282015%29011-e [Accessed 4 October 2025], para 27.

131 European Parliament and Council, 2016., Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities…' (Law Enforcement Directive). *Official Journal of the European Union*, L 119, 4 May, 89–131. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680 [Accessed 4 October 2025], paras 33-40.

132 See in general, Den Boer, M., 2018. 'Police oversight and accountability in a comparative perspective'. In: B. Hebenton and T. Maljevic, eds. *Comparative Policing from a Legal Perspective*. Berlin: Duncker & Humblot, 443–464; Den Boer, M. and Van Buuren, J., 2012. 'Security clouds: Towards an ethical governance of surveillance in Europe'. *Journal of Cultural Economy*, 5/1, 85–103.

2. *Post 9/11 Era*. The paradigm of the intelligence services, law enforcement and criminal law changed, shifting from reactive to proactive in terms of gathering data. Their paradigm shifted towards fusion which can be seen in joint terrorism task forces, fusion centres. In the same period intelligence-led policing models merged operational lines. The police increasingly became both producers and consumers of intelligence and gathered evidence which contributed to greater integration between the agencies.

3. *Digital Era.* In the digital era, regulation means a more practical approach and the EU Directive 2023/977 is a key instrument. This Directive established harmonized rules for the adequate and rapid exchange of information between the competent law enforcement authorities of the EU Member States, i.e. to create a *single point of contact* for efficient police-to-police information exchange, institutionalizing cross-border criminal-intelligence workflows.[133]

Evidently the dynamics of the structure are gaining more of a proactive approach. However, despite these structural shifts, in many systems, intelligence officers remain barred from collecting courtroom-admissible evidence in order to preserve procedural fairness and to avoid disclosure of covert methods.[134]

The Venice Commission is the Council of Europe's advisory body on constitutional law and thus provides legal advice to member states on constitutional and democratic reforms. The Commission has warned that signals-intelligence agencies, often the most powerful and best resourced, continue to operate with less legislative scrutiny than traditional law-enforcement bodies, creating potential accountability gaps in areas of mass surveillance.[135] New models of multi-agency accountability and enhanced roles for data-protection authorities will be necessary in monitoring these cross-cutting data environments.[136] However, the integration of Artificial Intelligence (AI) into law enforcement and intelligence practices will be the next major challenge. Here the use of open-source intelligence, commercial datasets, and classified data raises complex questions about transparency, oversight, and legal safeguards that current regulatory instruments only partially address.[137]

133 European Parliament and Council, 2023. 'Directive (EU) 2023/977 of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States…' *Official Journal of the European Union*, L 134, 1–24. Available at: https://eur-lex.europa.eu/eli/dir/2023/977/oj/eng [Accessed 4 November 2025], paras, 33-40.

134 Damaška, M., 2001. *Dokazno pravo u kaznenom postupku: oris novih tendencija*. Zagreb: Pravni fakultet u Zagrebu.

135 European Commission for Democracy through Law (Venice Commission), 2015.

136 Karas, Ž., 2012. 'Neke primjedbe o izdvajanju nezakonitih materijalnih dokaza'. *Policija i sigurnost* 21/4, 753–774.

137 Situmeang, S., Mahdi, U., Zulkarnain, P., Aziz, H. and Nugroho, T., 2024. 'The Role of Artificial Intelligence in Criminal Justice'. *Global International Journal of Innovative Research* 2, 1966–1981. Available at: https://www.researchgate.net/publication/383779490_The_Role_of_Artificial_Intelligence_in_Criminal_Justice [Accessed 4 November 2025], 1970.

2.2.3. Oversight and accountability mechanisms

Legislative, executive and judicial oversight is the cornerstone of democratic accountability for the intelligence sector. The institutional design and the function of legislative oversight bodies has the same function. However, its operationalization differs significantly in the United States and Europe in terms of structural strengths, jurisdiction and limitations in their ability to monitor, restrain, and shape intelligence activity in accordance with rule of law principles.

2.2.3.1. Parliamentary committees and special commissions: Ensuring legislative scrutiny

U.S. Congressional oversight of the intelligence community is institutionally concentrated in two standing committees with broad authority: the House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI).[138] Furthermore, the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence review intelligence budgets, investigate abuses or failures, hold hearings (public and classified), and issue reports. Johnson discusses both strengths and weaknesses here. Strengths include the committees' investigative powers and capacity for reform; while among weaknesses are political polarization, secrecy, and the tendency of Congress to defer to executive branch prerogatives, especially in times of crisis.[139] These bodies shape and draft the annual Intelligence Authorization Act, checking and approving covert-action operations. They regularly review confidential reports from the agencies' internal watchdog and classified reports from agency Inspectors General.[140] Furthermore, while the Intelligence Authorization Act provides Congress with oversight tools, congressional oversight in practice has yielded both major successes and notable failures. For example, the Church Committee's investigations in the 1970s exposed widespread abuses and led to historic reforms, while congressional inquiries into the Iran-Contra affair forced greater transparency and accountability. However, oversight has sometimes faltered, such as when Congress failed to challenge flawed intelligence on Iraq's weapons of mass destruction or did not adequately scrutinize controversial CIA interrogation and NSA surveillance programs. Indeed, the full extent of these actions only became evident with external disclosures.[141]

138 Albanesi, E., 2021. 'Models of Parliamentary Scrutiny of the Quality of Legislation: How Different Drafting Models and Forms'. Available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/thorceleg9&div=11&id=&page= [Accessed 4 October 2025].

139 Johnson, L.K., 2017. *Spy Watching: Intelligence Accountability in the United States*. Oxford: Oxford University Press.

140 United States Congress, 2022. Intelligence Authorization Act for Fiscal Year 2023, Public Law No. 117–263, U.S. Statutes at Large. Available at: https://www.congress.gov/bill/117th-congress/house-bill/7776/text [Accessed 4 October 2025], sec. 402.

141 Johnson, L.K., 2017. *Spy Watching.*

On the other hand, European parliamentary oversight is decentralized and structurally diverse, reflecting national traditions and legal cultures. In national jurisdictions, such as the U.K., Germany, and the Netherlands the mechanisms are quite different. In the United Kingdom, for example, the cross-party Intelligence and Security Committee (ISC),[142] although independent on paper, operates under Cabinet Office constraints; its 2022–2023 report explicitly noted that there is a lack of oversight for intelligence and security activities conducted by certain policy departments, such as the Ministry of Defence, the Cabinet Office, and the Home Office. The Committee emphasized that this gap prevents the effective scrutiny of national security issues, contravening commitments made to Parliament.[143] On the other hand, Germany's *Parlamentarisches Kontrollgremium* (PKGr)[144] receives quarterly briefings from the executive but lacks subpoena power and cannot compel witness testimony, relying largely on the executive's discretion for access to classified materials (Deutscher Bundestag). In contrast, the Dutch parliament possesses formal inquiry and subpoena powers under Article 70 of the Dutch Constitution and the Parliamentary Inquiry Act.[145] This allows either chamber (House of Representatives or Senate) to establish a parliamentary inquiry, summon witnesses compel the production of documents, and place witnesses under oath.

Germany and the Netherlands's parliamentary oversight of intelligence operations is mainly retrospective, with committees briefed only after actions have been taken. There is generally no power for parliaments to approve or block intelligence activities in advance. In Germany and the Netherlands, any *ex-ante* oversight occurs at the judicial or administrative, not the parliamentary level. Across Europe, true *ex-ante* parliamentary review is extremely rare; notable exceptions are Norway, where a parliamentary committee can sometimes review operations before they happen, and Sweden, where judicial authorization is required for surveillance, but not by parliament.

To address potential misconduct or to conduct more in-depth investigations, the German Bundestag has the authority to establish parliamentary inquiry committees (*Untersuchungsausschüsse*). These committees are endowed with broader powers, including the ability to summon witnesses and collect evidence, thereby providing

142 ISC is a UK parliamentary body that oversees the work of the country's intelligence agencies, ensuring that they are accountable to Parliament.

143 Intelligence and Security Committee of Parliament, 2023. *Annual Report 2022–2023. HC 287. Presented to Parliament pursuant to sections 2 and 3 of the Justice and Security Act 2013.* London: The Stationery Office. Available at: https://isc.independent.gov.uk/wp-content/uploads/2023/12/ISC-Annual-Report-2022-2023.pdf [Accessed 4 October 2025], 15.

144 This body is Germany's parliamentary oversight committee for the intelligence services. It monitors and reviews the activities of agencies like the BND, BfV, and MAD to ensure they act within the law and remain accountable to Parliament.

145 Grondwet voor het Koninkrijk der Nederlanden [Constitution of the Kingdom of the Netherlands], Art. 70; *Wet op de parlementaire enquête 2008* [Parliamentary Inquiry Act 2008], Stb. 2008, 605. Available at: https://wetten.overheid.nl/BWBR0023825/2022-05-01 [Accessed 4 October 2025].

a more robust mechanism for oversight when necessary.[146] The Netherlands, however, offers a more interventionist and U.S. based model: the CTIVD.[147] The CTIVD, a parliamentary accountability body, is not only empowered to conduct retrospective audits but, under the 2023 Temporary Act, can order intelligence services to delete unlawfully obtained data. This decision is binding unless overturned by the highest administrative court, offering a rare instance where a legislative oversight body holds a direct veto over operational legality.[148]

At the EU level, oversight has taken a distinct and more elaborate form. A striking example is the European Parliament's PEGA Committee, established in response to the Pegasus spyware scandal. Pegasus, developed by NSO Group, had been deployed against journalists, activists, and politicians, prompting the European Parliament to investigate the scale of the abuse and to propose safeguards for digital rights and privacy. What began as an inquiry into commercial spyware quickly evolved into a broader reflection on how the democratic oversight of intelligence should function in an age when off-the-shelf surveillance tools can threaten journalism, dissent, and even elections. In its 2023 report, the PEGA Committee urged harmonised export controls, remedy rights for those targeted, and cross-border accountability mechanisms to prevent intelligence actors from evading scrutiny behind national borders.[149]

2.2.3.2. Judicial oversight: Courts, warrants, and the review of intelligence-led operations

Through mechanisms such as judicial review, the issuance of warrants, and court-supervised procedures, the judiciary acts as a check on intelligence agencies whether in national emergencies or in complexed criminal proceedings. This oversight is designed to uphold individual rights and procedural fairness, but also to strengthen public trust in the rule of law, as secret or coercive methods are often employed in the name of national security.

146 Heumann, S. and Wetzling, T., 2014. Strategische Auslandsüberwachung: Technische Möglichkeiten, rechtlicher Rahmen und parlamentarische Kontrolle. Policy Brief. Berlin: Stiftung Neue Verantwortung. Available at: https://www.interface-eu.org/storage/archive/files/052014_snv_policy_brief_strategische_auslandsuberwachung.pdf [Accessed 2 October 2025], 15.

147 The Dutch Committee on the Inteligence and Security Sevices oversees the activities of the Netherlands' intelligence agencies, namely the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD). Its primary responsibilities include assessing the legality of these agencies' operations and handling complaints related to their conduct.

148 Review Committee on the Intelligence and Security Services (CTIVD), 2024. *Annual Report 2023*. Available at: https://english.ctivd.nl/latest/news/2024/09/26/index [Accessed 4 November 2025], 15-19.

149 European Parliament, 2023. *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://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.html, [Accessed 4 October 2025].

Judicially-speaking, oversight of intelligence is grounded in fundamental rights law. Any surveillance measure must be grounded on the ECtHR established principles of *necessity in a democratic society,* proportionality, and legality. The principle of necessity in a democratic society pertains to how any restriction on rights envisaged in the ECHR must be essential, proportionate, and justified by a pressing social need, not just useful or desirable. It requires governments to show that a limitation serves a legitimate aim and is strictly required to protect democracy, as interpreted by courts like the ECtHR. Surveillance measures must be proven necessary to protect national security or public safety, not simply convenient for authorities. For instance, EU data protection laws (like GDPR) also indirectly constrain intelligence activities, as seen in the *Schrems* cases.[150] The U.S. approach is, in contrast, rooted in national security concerns and a thorough distinction between U.S. citizens and foreign nationals and the different treatment of the two. The Fourth Amendment to the U.S. Constitution protects citizens against unreasonable searches and requires judicial approved warrants based on probable cause. However, it offers no protection to non-U.S. persons abroad. Intelligence gathering on foreign targets is authorized by statutes like the Foreign Intelligence Surveillance Act (FISA Act)[151] and the USA PATRIOT Act,[152] which expanded national security surveillance powers in the post 9/11 era. The common nominator of these laws is prioritizing security needs first by allowing broad data collection (e.g. bulk telephony metadata) to be collected with fewer individualized protections than typically required for criminal investigations.[153] After public controversies over surveillance, the U.S. has imposed tighter controls on the collection of metadata from non-U.S. persons abroad. Laws such as the Presidential Policy Directive 28,[154] USA FREEDOM Act,[155] and reforms to FISA have introduced new restrictions and increased oversight. They require greater justification, minimization, and transparency in intelligence practices, even when collecting data on non-U.S. persons overseas.

150 Together, these rulings established that any international data transfer regime must offer "essentially equivalent" protections to those guaranteed within the EU. The decisions have had far-reaching consequences for global data governance, compelling organizations to reassess compliance with EU data protection standards and prompting further transatlantic negotiations on a new data transfer framework. Schrems I: Court of Justice of the European Union. (2015). *Maximillian Schrems v Data Protection Commissioner* (Case C-362/14, Judgment of 6 October 2015). *ECLI:EU:C:2015:650.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362 and Schrems II: Court of Justice of the European Union. (2020). *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (Case C-311/18, Judgment of 16 July 2020). *ECLI:EU:C:2020:559*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311.

151 U.S. Congress, 1978. *Foreign Intelligence Surveillance Act of 1978*, *Pub. L. No. 95-511, 92 Stat. 1783, codified as amended at 50 U.S.C. §§ 1801–1885c*. Available at: https://www.law.cornell.edu/uscode/text/50/chapter-36, [Accessed 4 October 2025].

152 U.S. Congress, 2001. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*, *Pub. L. No. 107-56, 115 Stat. 272*. Available at: https://www.congress.gov/bill/107th-congress/house-bill/3162 [Accessed 4 October 2025].

153 U.S. Congress, 2001. *Uniting*, 215.

154 The White House, 2014. *Presidential Policy Directive/PPD-28: Signals Intelligence Activities*, 17 January. Washington, D.C.

155 United States Congress, 2015. *USA FREEDOM Act of 2015, Public Law 114–23*. Washington, D.C.: Government Printing Office.

Models of review

When it comes to the judicial review models, a key difference is made along the lines of *ex-ante vs. ex-post oversight*.[156] Parliamentary oversight of emergency powers in Germany is more robust than in many European systems, as the German Basic Law requires explicit Bundestag approval to declare a state of defence or internal emergency, and limits the executive's authority through strong judicial review and parliamentary committees. In contrast, some countries such as France and the UK allow the executive greater leeway to act in emergencies, with parliament only being informed or consulted after the fact. German emergency procedures include: formal declarations of a state of defence or internal emergency; possible transfer of legislative power to the Joint Committee if parliament cannot convene; strict limits on deploying the military domestically; and the continued protection of core constitutional rights, ensuring checks and balances even in crisis situations.[157] Many European systems rely on *prior judicial or independent authorization* for surveillance as a measure of protection for the right of privacy. Interception of communications always requires a court warrant or an independent body before intelligence agencies proceed with the gathering of data.[158] The independent body system is seen in the Netherlands. Here the Intelligence Act 2017 established the Review Board (TIB) to *ex-ante*-authorize surveillance warrants, while another (separate) Review Committee (CTIVD) provides *ex post facto* oversight.[159] In much the same way, Germany's G10 Commission (which is also an independent body chaired by a judge) must approve signals intelligence measures in advance, except in emergencies, and regularly reviews ongoing operations.[160] The law authorizes the G10 Commission, an independent oversight body, to assess and authorize surveillance measures proposed by Germany's federal intelligence services: the Federal Intelligence Service (BND), the Federal Office for the Protection of the Constitution (BfV), and the Military Counterintelligence Service (MAD).

156 *Ex-ante oversight* occurs before an action is taken, for example, requiring judicial authorization prior to surveillance. *Ex-post oversight* takes place after the action, such as parliamentary reviews, audits, or court proceedings examining the legality or proportionality of already-conducted operations. Both are essential for ensuring legality and democratic control, especially in contexts involving privacy or surveillance.

157 Bundesverfassungsgericht (BVerfG), 2020. Urteil des Ersten Senats vom 19. Mai 2020 – 1 BvR 2835/17. Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rs20200519_1bvr283517.html [Accessed 4 October 2025]

158 Nino, M., 2007. 'The Abu Omar Case in Italy and the effects of CIA renditions in Europe on Law Enforcement and Intelligence Activities'. *Revue Internationale de Droit Pénal* 78/1–2, 113–141.

159 This Act, Government of the Netherlands, 2017. *Wet op de inlichtingen – en veiligheidsdiensten* 2017 [Intelligence and Security Services Act 2017]. Staatsblad van het Koninkrijk der Nederlanden, 317. Available at: https://english.aivd.nl/about-aivd/the-intelligence-and-security-services-act-2017, [Accessed 4 October 2025], expanded the powers of the Dutch intelligence and security services, including provisions for bulk data collection, hacking, and international data sharing, while introducing oversight mechanisms such as the Review Board for the Use of Powers (TIB) and the Review Committee for the Intelligence and Security Services (CTIVD)

160 Federal Republic of Germany, 1968. *Gesetz zur Beschränkung des Brief-, Post – und Fernmeldegeheimnisses* [Act to Restrict the Privacy of Correspondence, Posts, and Telecommunications] (BGBl. I S. 949), last amended by Article 4 of the Act of 22 December 2023 (BGBl. I S. 3775). [Accessed 4 October 2025].

In the U.S. oversight has traditionally been more *ex-post*. The FISA Act created the U.S. Foreign Intelligence Surveillance Court[161] to approve surveillance targeting foreign powers or agents, but these proceedings are *ex parte* and classified, in which only representatives of the government are present at the secret trial. So FISC operates *ex-ante* by issuing warrants, and its hearings lack adversarial debate. This is different from the ordinary U.S. courts which typically become involved only *after* surveillance has occurred: for instance, if evidence gathered by intelligence is used in a trial. However, focusing solely on *post-facto* accountability in U.S. wiretapping overlooks how groundbreaking and far-reaching the *ex-ante* warrant requirement introduced by FISA (1978) truly was, setting the U.S. apart globally.[162] Ongoing reforms, especially after the Snowden revelations, have further strengthened these *ante facto* safeguards and expanded judicial oversight.

The FISC operates primarily on an *ex-ante* basis, requiring authorities to secure a warrant before initiating a wiretap. In many areas, the U.S. is unique in mandating such prior judicial oversight, even for sensitive covert actions[163] Additionally, recent reforms have introduced a limited adversarial process within FISC proceedings.

Divergent approaches

In *Clapper v. Amnesty International*[164] the U.S. Supreme Court denied plaintiffs from challenging secret surveillance under FISA, as they could not prove they were personally affected. The Supreme Court, in a 5–4 decision, dismissed the case on the grounds of standing. The Court emphasized that a chain of hypothetical future events does not meet the requirement of a concrete and particularized injury under Article III of the Constitution. The importance of this decision is seen in the significant limitation of the ability of individuals to bring legal challenges against secret surveillance programs, reinforcing the government's discretion in national security matters and highlighting the challenges of ensuring judicial accountability in intelligence oversight. This further highlights the *post-facto* accountability gap in the U.S. indicating that potential victims struggle to obtain judicial review because of secrecy requirements.[165]

161 These special courts or FISCs are composed of federal judges appointed to review government applications for electronic surveillance and searches in national security cases. FISC proceedings are classified and its secrecy is justified by the need to protect sensitive intelligence sources in the name of national security.

162 U.S. Congress, 1978. *Foreign Intelligence Surveillance Act*.

163 Johnson, *The Third Option*, 2022, OUP.

164 U.S. Supreme Court, 2013. *Clapper v. Amnesty International USA, 568 U.S. 398*. Available at: https://supreme.justia.com/cases/federal/us/568/398/ [Accessed 4 October 2025].

165 Global Freedom of Expression, 2013. Clapper v. Amnesty International USA. Columbia University. Available at: https://globalfreedomofexpression.columbia.edu/cases/clapper-v-amnesty/ [Accessed 4 October 2025].

European experiences are different. Both national courts and the supranational courts (ECtHR/CJEU) have been more open to reviewing surveillance laws and requiring *ex ante* safeguards. European courts emphasize that independent authorization and oversight (preferably judicial) must oversee surveillance from the start through to the after-the-fact review. In Europe, there is generally no exact analogue of the secret FISC courts in the U.S., but instead, judicial or semi-judicial bodies handle intelligence oversight depending on the context. Most European countries entrust surveillance warrants to regular criminal law judges or special panels and allow subsequent challenges in constitutional or administrative courts. Germany's Federal Constitutional Court has several landmark rulings on intelligence activities, acting as a check on legislation. This approach would be considered as a strength because it is able to better evaluate the merits of the case. The Constitutional Court ruling on the Foreign Intelligence Service Act emphasized that even foreign intelligence operations must adhere to fundamental rights and required the introduction of clear legal boundaries and independent oversight to prevent abuses and protect privacy.[166]

Jurisprudence of the ECtHR and CJEU

In *Zakharov v. Russia*, where The Court set strict standards for surveillance laws, emphasizing that secret measures must have adequate and effective guarantees against abuse, such as independent authorization and the possibility of later review. The ECtHR found Russia's broad interception system violated Article 8 due to lack of effective judicial supervision. Furthermore, it stressed that effective safeguards against abuse are essential: safeguards could include prior judicial authorization, post-surveillance notification, and access to remedies. The safeguards should be in line with equality of law doctrine, requiring that surveillance laws be accessible, foreseeable, and limited in scope to prevent arbitrary interference by state authorities.[167]

In *Big Brother Watch v. UK,* the Court reviewed the UK's post-Snowden bulk interception regime and held that bulk surveillance of communications can be compatible with the Convention only in case of existence of 'end-to-end safeguards' which further ensure independent authorization, ongoing supervision, and *ex-post* review.[168] The Court reasoned that that national security cannot be used as a

166 Bundesverfassungsgericht (BVerfG), 2020. *Urteil des Ersten Senats vom 19. Mai 2020 – 1 BvR 2835/17*. Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rs20200519_1bvr283517.html [Accessed 4 October 2025].

167 European Court of Human Rights, 2015. Zakharov v. Russia, no. 47143/06, Grand Chamber, Judgment of 4 December 2015. Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159324%22 [Accessed 4 October 2025].

168 Public International Law & Policy Group, 2021. 'Big Brother Watch v. the United Kingdom: A trend towards accepting surveillance regimes in Europe'. *Lawyering Justice Blog*, 6 September. Available at: https://www.publicinternationallawandpolicygroup.org/lawyering-justice-blog/2021/9/6/big-brother-watch-v-the-united-kingdom-a-trend-towards-accepting-surveillance-regimes-in-europe, [Accessed 4 October 2025].

blanket justification for disproportionate interference with fundamental rights. This means that even in cases where states pursue legitimate security objectives, the legal measures governing surveillance must include precise rules, judicial control, and effective remedies. In this case the UK had allowed executive discretion to approve bulk data taps, which the Court found deficient and in violation of Articles 8 and 10 of the Conviction. Insufficient judicial control and protections for confidential journalist communications were noted.[169]

CJEU is relevant for the notable decisions in the Schrems trilogy. Schrems I challenged the validity of the EU-U.S. Safe Harbor framework, which allowed companies like social media giants Meta, Apple, X based in Ireland to transfer personal data to the U.S. The CJEU agreed and struck down the Safe Harbor agreement, ruling that it lacked sufficient safeguards and effective legal remedies for EU citizens, and the guarantees they enjoyed under EU law.[170] This action led to the adoption of a new framework, namely the EU–U.S. Privacy Shield. This was contested by the Schrems II judgment, over the legitimacy of the Privacy Shield and the use of Standard Contractual Clauses (SCCs) for transferring data to the U.S. The CJEU once again invalidated the transatlantic framework concluding that U.S. FISA Act Section 702 and Executive Order 12333 permitted disproportionate access to personal data and did not offer individuals effective redress mechanisms.[171] This new agreement introduced a set of reforms, including the establishment of a Data Protection Review Court in the U.S. and updated commitments by intelligence authorities. This court is a specialized U.S. body established in 2023 required to review and adjudicate complaints coming from non-U.S. individuals regarding the misuse of their personal data by U.S. intelligence agencies. It provides an independent legal remedy and oversight mechanism for transatlantic data privacy disputes, particularly under the EU-U.S. Data Privacy Framework.[172] The CJEU's judgments, especially in 2020, reaffirmed strict limits on government-mandated data retention by telecommunications providers. The judgements also emphasized that broad, indiscriminate data collection is generally incompatible with EU fundamental rights to privacy and data protection.[173]

169 European Court of Human Rights, 2021. *Big Brother Watch and Others v. the United Kingdom, nos. 58170/13, 62322/14 and 24960/15, Grand Chamber, Judgment of 25 May 2021*. Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-210077%22]} [Accessed 4 October 2025].

170 Public International Law & Policy Group, 2021. 'Big Brother Watch'.

171 Executive Order No. 12333*: United States intelligence activities*, 46 Fed. Reg. 59941 (Dec. 4, 1981). Available at: https://www.archives.gov/federal-register/codification/executive-order/12333.html. [Accessed 4 November 2025]

172 U.S. Department of Commerce, 2023. *Data Privacy Framework Program Overview*. Available at: https://www.dataprivacyframework.gov/Program-Overview [Accessed 4 October 2025].

173 Eskens, S., 2022. 'The ever-growing complexity of the data retention discussion in the EU: An in-depth review of La Quadrature du Net and Others and Privacy International'. European Data Protection Law Review, 8/1, 143–155. Available at: https://edpl.lexxion.eu/article/EDPL/2022/1/22 [Accessed 4 October 2025].

2.2.3.3. Executive supervision: The role of Ministries, National Security Advisors, and Presidential Bodies

In the U.S. executive supervision is marked by executive privilege and secrecy.[174] The executive branch can and does invoke the *state secrets privilege* to block litigation that might reveal classified programs. Oversight bodies (like congressional intelligence committees and the FISC) operate in non-public manner with the appointment of *amici curiae* to represent privacy interests. In Europe, the situation is different. While intelligence operations are inherently classified, there is a well-established tradition, grounded in the jurisprudence of the ECtHR and the CJEU, requiring that surveillance laws be sufficiently clear, foreseeable, and publicly accessible in accordance with the principle of legality, and that individuals have an avenue for redress, even if only ex post facto through an oversight body or a court. However, Europe is not immune to excessive secrecy – many national security proceedings happen *in camera*.[175] Furthermore, the influence of whistleblowers should not be underestimated. The Edward Snowden's 2013 revelations about NSA and GCHQ surveillance reverberated through Europe, leading directly to court challenges (*Big Brother Watch*, *Schrems*, etc.) and legislative reforms. Those scandals prompted Germany and France to pass new laws to legalize or constrain mass surveillance with added oversight (albeit controversially), and the EU forged new data-transfer accords with the U.S. that include oversight provisions.[176] These laws still allowed for sweeping interception of communications, insufficient transparency, and limited judicial or parliamentary control, raising concerns about privacy rights and the adequacy of independent oversight. Civil society groups and data protection advocates warned that, despite formal safeguards, the reforms often prioritized national security at the expense of fundamental rights.

2.2.3.4. Media and whistleblowers: Informal accountability mechanisms, case studies from the Euro-Atlantic region

Democratic oversight of intelligence services almost always relies on formal mechanisms such as parliamentary committees and ombudsmen. However, informal accountability through investigative journalism and whistleblowers has become increasingly important in holding intelligence agencies to account. Here we will look at cases from Poland, Finland, Croatia and the Netherlands, where media revelations and insider leaks have exposed secret surveillance programs, abuses of power, and legal gaps, often prompting reforms.

174 Hillebrand, C., 2013. 'Intelligence oversight and accountability'. In: M. Phythian, ed. Routledge *Companion to Intelligence Studies*. London: Routledge, 305–312.

175 Rittberger, B. and Goetz, K.H., 2018. 'Secrecy in Europe'. *West European Politics* 41/4, 825–845. Available at: https://www.tandfonline.com/doi/full/10.1080/01402382.2017.1423456 [Accessed 4 October 2025].

176 Court of Justice of the European Union, 2015. *Maximillian Schrems v Data Protection Commissioner*.

Poland

Poland's intelligence sector is formally overseen by a Parliamentary Committee for Special Services and internal controls. In practice, oversight has been weak and highly politicized. Court warrants are required for wiretaps, but judges rarely refuse them, and targets are not notified post-surveillance.[177] Reforms ordered by a 2014 Constitutional Tribunal ruling and a 2016 Venice Commission opinion were largely ignored[178] and, instead, a 2016 anti-terror law expanded surveillance powers (e.g. allowing warrantless spying on foreign nationals) and dismantled safeguards. This law granted the Internal Security Agency (ABW) the authority to conduct warrantless surveillance on foreign nationals for up to three months if they were suspected of involvement in terrorist activities. Further this surveillance could be initiated without prior judicial approval. Poland's Ombudsman and civil society have repeatedly warned that citizens lack effective legal remedies against unlawful spying – a concern now at the ECtHR.[179] However, media and whistleblowers using the Polish media have uncovered major intelligence scandals. Notably, the Pegasus spyware affair ('Polish Watergate') erupted when investigative outlets and Citizen Lab revealed that, 2017-2019, the government had purchased NSO Group's Pegasus malware and used it to hack hundreds of phones, including the phones of opposition figures.[180] In late 2021, media reports from Politico identified Pegasus targets. These included an opposition campaign chief, lawyers, an independent prosecutor, public auditors, and even ex-ruling party officials.[181] These revelations came not from parliamentary scrutiny but through the work of journalists, whistleblowers, and NGOs.

Finland

Finland, long ranked among the world's freest and least corrupt countries, historically had limited intelligence capabilities and strict privacy protections. Around 2010, Finnish law still lacked comprehensive legislation for intelligence gathering, partly due to constitutional constraints. Security threats prompted change there, and by 2019 Finland enacted new Intelligence Laws that granted its civilian and military intelligence agencies broader surveillance powers (e.g.

177 Grabowska-Moroz, B., 2024. 'The Pegasus scandal in Poland – between old problems with state surveillance and the current rule of law crisis'. *about:intel*, 16 January. Available at: https://aboutintel.eu/pegasus-and-the-rule-of-law-crisis-in-poland/ [Accessed 2 October 2025].

178 Venice Commission, 2024. *Report on a Rule of Law and Human Rights Compliant Regulation of Spyware. CDL-AD(2024)043, adopted at the 141st Plenary Session* (Venice, 6–7 December 2024). Strasbourg: Council of Europe. Available at: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2024)043-e [Accessed 2 October 2025].

179 Amnesty International, 2016. *Counter-terrorism bill would give security service unchecked power*. EUR 37/4263/2016. Available at: https://www.amnesty.org/en/documents/eur37/4263/2016/en/. [Accessed 2 October 2025]

180 Grabowska-Moroz, B., 2024. 'The Pegasus scandal'.

181 Kość, W., 2024. 'Poland launches Pegasus spyware probe'. *POLITICO*, 19 February. Available at: https://www.politico.eu/article/poland-pegasus-spyware-probe-law-and-justice-pis-jaroslaw-kaczynski/ [Accessed 2 October 2025].

signals intelligence) with oversight structures.[182] Further, the Finish Parliament amended the Constitution to allow surveillance of communications for national security and set up an Intelligence Oversight Committee (a parliamentary committee) and an independent Intelligence Ombudsman.[183] These bodies supervise legality and handle complaints, adding to Finland's existing oversight (the Parliamentary Ombudsman and Data Protection Supervisor also oversee certain aspects). Thus, since 2019 Finland has a relatively robust formal oversight framework, at least on paper. Nonetheless, the tension between Finland's commitment to an open society and the secrecy of security operations has come to the fore in recent years, revealing that even in Nordic democracies, intelligence oversight can be contentious.[184]

However, the most significant episode testing Finland's balance of press freedom and secrecy was the Helsingin Sanomat case. This involved Finnish journalists convicted in January 2023 for revealing classified defence intelligence in a 2017 article about the Finnish Intelligence Research Centre. In its ruling the court acknowledged the information was indeed sensitive to national security.[185] Crucially, the journalists had argued the material was already partly public and that their reporting served the public interest (coming amid legislative debates). Press freedom organizations condemned the convictions, calling them a "dangerous precedent" given Finland's top-tier press freedom status.[186] They warned that if Finland imprisons or fines journalists for such reporting, it could embolden more repressive states.[187] The case marked the first time since WWII that Finnish reporters faced criminal sentences for publishing leaked information.

Apart from this case, Finland has not seen high-profile whistleblowers leaking from within intelligence agencies (which are relatively small). However, it is likely that *some* insider provided the documents to the national newspaper, *Helsingin Sanomat* – an act of whistleblowing without formal protection. Finland did implement a Whistleblower Protection Act in 2023 [188] by transposing the EU Directive, which protects disclosures of wrongdoing in many sectors. National security and defence secrets, though, remain excluded from such protections, as is common across Europe. Thus, an intelligence employee in Finland must report

182 Lohse, M., 2023. 'Finnish intelligence overseers' right of access supersedes Originator Control'. *about:intel*, 23 October. Available at: https://aboutintel.eu/finnish-intelligence-overseers-right-of-access-supersedes-originator-control/ [Accessed 2 October 2025].

183 Widlund, J., 2022. 'More Than Just Blind Guardians? A Legal Analysis of Finnish Parliamentary Oversight of Intelligence'. *Scandinavian Studies in Law* 69, 66–89. Available at: https://scandinavianlaw.se/pdf/69-4.pdf [Accessed 2 October 2025].

184 Lohse, M., 2023. 'Finnish intelligence overseers' right of access supersedes Originator Control', 21-25.

185 AP News. 2025. *3 Finnish journalists on trial for revealing defense secrets*. AP News. Available at: https://apnews.com/article/journalists-denmark-newspapers-military-intelligence-41ed011af240f80accf883c021d4701d [Accessed 2 October 2025].

186 AP News, 2025.

187 Al Jazeera, 2022. *Finland puts journalists on trial for revealing defence secrets*. Al Jazeera. Available at: https://www.aljazeera.com/news/2022/8/25/finland-puts-journalists-on-trial-for-revealing-defence-secrets [Accessed 2 October 2025].

188 Finland, 2022. Whistleblower Protection Act (1171/2022). Available at: https://www.finlex.fi/fi/lainsaadanto/saadoskokoelma/2022/1171 [Accessed 2 October 2025].

concerns internally or to oversight bodies like the Intelligence Ombudsman rather than to the media. The Ombudsman role, created in 2019, offers a legal channel for reporting improper intelligence activities confidentially. It remains to be seen how frequently insiders use this channel (Intelligence Ombudsman 2025).[189] The Intelligence Ombudsman has the mandate to ensure intelligence operations comply with law and that they can receive whistleblower tips confidentially. It is possible that if such structures had been there earlier, journalists would not have felt the need to publish classified details to stimulate parliamentary debate.

Croatia

Croatia completely reformed its security apparatus in the early 2000s as it transitioned from the post-Yugoslav era and sought EU/NATO membership. It established multiple oversight layers: a standing parliamentary committee on national security, a civilian *Council for Civilian Oversight of Security and Intelligence Agencies*, and an Office of the National Security Council.[190] The seven-member civilian Council (appointed by its parliament and restricted to non-partisan professionals) can inspect the legality of agency operations and handle citizen complaints about rights. These mechanisms are meant to ensure intelligence agencies (the Security and Intelligence Agency, SOA, and Military Security Agency, VSOA) remain accountable. In practice, however, Croatia's oversight bodies often operate *in camera*, and their effectiveness has been questioned. Political influence lingered – especially in the early 2010s – as intelligence posts and inquiries could split along party lines.[191]

The Croatian press and whistleblowers have played a role in prodding oversight, albeit in a few notable cases. In 2014, a scandal erupted when an SOA officer-turned-whistleblower leaked classified documents exposing internal employment irregularities (e.g. including nepotistic or unlawful hires within the agency).[192] The revelations, published in the media, forced the Croatian parliament's security committee to investigate. The inquiry's outcome, however, broke down along partisan lines – ruling coalition MPs versus opposition – suggesting a reluctance by those in power to limit or punish the service.[193] Nonetheless, the incident raised public awareness about intelligence accountability and likely spurred the agency to tighten internal controls. It is worth noting that the Croatian media had reported on

189 Tiedusteluvalvonta. (n.d.). *Front page* [Website]. Available at: https://tiedusteluvalvonta.fi/en/home? [Accessed 2 October 2025].

190 Lozančić, D., 2020. *Insights and Lessons Learned from Croatia's Intelligence Reforms*. Geneva: DCAF. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/ECA_Paper_Intelligence_Reform_Oct2020.pdf [Accessed 2 October 2025].

191 Lozančić, 2020. *Insights*.

192 Whistleblowing International Network. (2021, April 9). *Open Letter to Croatian Minister of Justice to free whistleblower Jonathan Taylor*. Available at: https://whistleblowingnetwork.org/News-Events/News/News-Archive/Open-Letter-to-Croatian-Minister-of-Justice-to-fre? [Accessed 2 October 2025].

193 Lozančić, 2020. *Insights*.

alleged abuses (from an earlier era, cases like journalists accusing a predecessor agency of harassment), creating pressure for reform.

Beyond that 2014 case, there have been fewer high-profile whistleblower leaks in Croatia's intelligence sphere post-2010 – a sign perhaps of tighter secrecy or less watchdog journalism in this area. One constraint was a culture of secrecy dating to the Yugoslav era; intelligence matters were long considered off-limits. This has gradually shifted as Croatia adopted international good practices. By the late 2010s, Croatia acknowledged the need to protect those exposing wrongdoing. Like Finland, Croatia also passed a Whistleblower Protection Act, its first comprehensive law to shield whistleblowers from retaliation.[194] The law was welcomed as progress, though it consisted of reporting procedures and uncertainty about coverage of national security issues. It is likely that disclosures involving classified security information still require special handling (or fall outside the standard law), something which may deter intelligence-sector whistleblowing.[195] Whistleblowers can now report misconduct through protected channels, though state security secrets remain sensitive. Press freedom in Croatia has improved since the 1990s, but journalists still face occasional pressures (e.g. defamation suits or political influence on media). Intelligence agencies generally avoid direct confrontation with journalists today, a change from earlier eras. But allegations of surveillance against journalists have surfaced in the region. Overall, Croatia's mix of formal oversight bodies and gradual cultural change – influenced by media scrutiny – has led to more transparency, though sustained vigilance will be necessary to assure this trend continues.

The Netherlands

The Netherlands employs a two-tier oversight system under its 2017 Intelligence and Security Services Act.[196] All proposed uses of special intelligence powers (e.g. wiretaps, bulk data interception) must receive prior approval from an independent Review Board (*Toetsingscommissie Inzet Bevoegdheden*, TIB).[197] The TIB conducts *ex-ante* judicial-style reviews of warrant requests already authorized by the relevant ministers, effectively acting as a check before surveillance begins. Its decisions are binding and if TIB denies approval, the operation cannot proceed. The oversight body (*CTIVD*, the Review Committee on Intelligence & Security) exercises *ex-durante* and *ex-post* oversight with extensive investigative powers.[198] The CTIVD audits the legality of intelligence operations and handles complaints, reporting its

194 Croatia, 2022. Zakon o zaštiti prijavitelja nepravilnosti [Act on the Protection of Persons Reporting Irregularities]. *Official Gazette* No. 46/2022. Available at: https://narodne-novine.nn.hr/clanci/sluzbeni/2022_04_46_572.html. [Accessed 2 October 2025]

195 Lozančić, 2020. *Insights*.

196 Government of the Netherlands, 2017. 'Wet op de inlichtingen'.

197 Government of the Netherlands, 2017.

198 Review Committee on the Intelligence and Security Services (CTIVD), 2024. *Annual Report* 2023.

findings to the Dutch parliament (often *via* public reports with classified annexes).[199] Notably, the CTIVD can review ongoing operations and those already concluded. However, under the current law its findings are not binding, though they carry weight and can prompt ministerial or parliamentary intervention. This dual structure (TIB and CTIVD) is unique and ensures that both preventive control (by TIB) and retrospective accountability (by CTIVD) are present. Dutch courts (administrative courts) can ultimately adjudicate complaints by citizens based on CTIVD reports. The Dutch approach illustrates a strong judicial oversight culture: independent experts pre-screen surveillance warrants for legality and proportionality, rather than leaving that solely to the executive.

2.2.4. Conclusion

Western European nations generally feature upfront judicial oversight (judges or independent commissions authorizing surveillance) and they have established external review bodies, although each country has unique structures. Eastern European countries have adopted many similar laws (warrant requirements, parliamentary committees), but in practice they often struggle with *executive override*, lack of resources for oversight bodies, and the political capture of institutions. Nonetheless, the effectiveness of oversight in Eastern Europe often hinges on broader rule-of-law conditions. The comparative lesson is that judicial oversight is crucial in tempering intelligence powers, and implementing such oversight remains an ongoing process across the region. Given the comparative findings, several reforms and trends can be identified to strengthen the judicial oversight of intelligence and better align security practices with rule of law and human rights standards:

Strengthen Judicial Authorization and Review. Surveillance programs – especially those involving bulk data collection or novel technologies – should be subject to judicial authorization by default. Furthermore, following the role of DCAF, judges involved in oversight should be given specialized training and security clearances to handle the complexities of intelligence cases, enabling them to ask the tough questions without unduly deferring to the government. On the *ex-post* side, providing individuals with a path to challenge surveillance (even if they only suspect they were subject to it) would enhance accountability. After all, this could include *notification provisions* (informing individuals after surveillance ends, as recommended by the Polish Constitutional Tribunal) and accessible complaint tribunals.

199 DCAF, 2011. *The Netherlands: Intelligence and Security Services Act, 2002*. Geneva: Geneva Centre for the Democratic Control of Armed Forces. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/Netherlands_EN.pdf [Accessed 2 October 2025].

Reform Secret Court Procedures. Secret courts and closed evidence procedures should be reformed to incorporate greater transparency and adversarial elements wherever possible. In the U.S., this means bolstering the FISC process. For instance, expanding the role of *amicus curiae* in FISC proceedings so that an independent voice is present in all significant cases, not just at the court's discretion. *Amici* (or special advocates) should be able to appeal FISC decisions or at least ensure the court hears privacy and civil liberty arguments. The secrecy of FISC rulings should be curtailed: publish redacted opinions by default and release historical decisions to build public jurisprudence. Legislative changes could mandate periodic declassification reviews of FISC opinions. In Europe, countries employing closed material should ensure the "gist" disclosure requirement is enshrined in statute.

Parliamentary and Independent Oversight Bodies. While this analysis focuses on judicial oversight, it is clear that judicial and parliamentary oversight go hand-in-hand. Countries should bolster the resources and powers of parliamentary intelligence committees and independent oversight authorities. Cooperation among oversight bodies should be enhanced – e.g., national oversight agencies in Europe could conduct *joint inquiries* into transnational surveillance operations (as intelligence sharing is now routine in EU and NATO contexts).

Adapting to AI Surveillance and Cyber Threats. Emerging technologies like AI, machine learning, and big data analytics are transforming intelligence surveillance. To address this, judicial and independent oversight bodies will need technical expertise, potentially *via* dedicated algorithmic audit units, to scrutinize datasets, code, and AI-driven decisions for bias or error. Legal standards may also need updating to explicitly cover AI-augmented surveillance.

Future Trends indicate that in the coming years will likely see continued judicial assertiveness, especially from European courts, in delineating the boundaries of acceptable surveillance. We might anticipate:

ECtHR Grand Chamber rulings that further refine the requirements for bulk interception oversight (several cases against European states' new laws are underway).

Further, CJEU judgments on encryption backdoors or government hacking practices might come out, which could impose EU-wide norms.

We might imagine national high courts intervening in real-time algorithmic surveillance. Meanwhile, legislatures will have to grapple with implementing these court decisions in workable statutes – a dynamic we already see in Germany post-BVerfG 2020, and in the UK post-ECtHR *Big Brother Watch*.[200]

200 BVerfG, 2020. *Urteil*; Public International Law & Policy Group, 2021. 'Big Brother Watch'.

2.3. The executive oversight of intelligence services

Grazvydas Jasutis and Kristina Vezon

2.3.1. Introduction

Executive oversight of intelligence services is a critical yet often undervalued dimension of democratic control. Executive supervision refers to the direct oversight and strategic direction exercised by the highest levels of the executive branch. Typically, ministries of defence or interior, national security councils, or the office of the president oversee intelligence agencies. In some countries, an Inspector General – usually established by law – supports the executive in overseeing intelligence services. These offices help ensure that agencies implement government policies properly and provide the executive with accurate, relevant information.[201] It does not encompass routine management tasks or interference into operational activities. Rather, it includes resource allocation and priority-setting, the alignment of intelligence operations with broader national security policies, legal frameworks, and democratic values.

The aim of this article is to offer a structural overview of executive oversight procedures, identify the institutions involved, and assess the challenges the executive oversight faces. Executive oversight remains insufficiently theorized, and a key dilemma remains unresolved. As Ian Leigh has stated:

> *too little control by the executive may be antidemocratic: intelligence becomes a law unto itself—a 'no go' zone. Moreover, without information or control ministers cannot be properly accountable to the public for this area of work. Where there is too much executive control the risk is that governments may be tempted to use security agencies or their exceptional powers or capacities to gather information for the purposes of domestic politics—for instance, to discredit domestic political opponents.*[202]

Hans Born and Ian Leigh in their book *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* state that unlike parliamentary and judicial forms of oversight, executive control is more immediate

201 Leigh, I., 2007. 'The accountability of security and intelligence agencies'. In: L.K. Johnson, ed. *Handbook of Intelligence Studies*. Abingdon: Routledge, 67–81.

202 Born, H., Johnson, L., Leigh, I. & Wills, A., 2011. *Who's Watching the Spies? Establishing Intelligence Service Accountability*. Washington, D.C.: Potomac Books.

and operational, involving direct tasking, prioritization, budgetary control, and appointment of intelligence leadership. However, their analysis also highlights the risks of excessive executive dominance, emphasizing the need for safeguards against ministerial abuse, such as clear laws, transparency mechanisms, and multi-actor oversight systems.[203] Leigh complements their study and explains that the executive's involvement in intelligence oversight carries two main risks: agencies becoming unaccountable, and politicians misusing them for partisan purposes. Democratic systems address these risks by maintaining executive control while safeguarding agencies from political abuse through ministerial oversight, reporting obligations, and formal written approvals. Covert operations, in particular, require strict executive authorization due to their sensitivity and potential for abuse. Effective oversight depends on a clear division between executive strategic direction and agency operational management. Over-involvement by political leaders can politicize intelligence and compromise its integrity.[204] Samuel J. Rascoff introduces the concept of 'presidential intelligence,' which describes the U.S. President's increasing role in actively overseeing intelligence collection. Rascoff argues that this trend reflects a broader centralization of executive power, paralleling the rise of presidential control in administrative law. He offers a cautious endorsement of this emerging model, proposing institutional designs to make it more effective and balanced.[205] Raab explores the role of the executive in shaping intelligence oversight, particularly through the institutions and legal frameworks that link ministers and intelligence services. He emphasizes the tension between political control and agency independence, noting the risks of either unchecked agency autonomy or the politicization of intelligence work by elected officials. Executive oversight is discussed in the context of ministerial responsibilities, such as approving covert actions, setting strategic directions, and receiving reports from intelligence agencies. Raab highlights how executive roles must be balanced by independent mechanisms, like inspectors general or parliamentary committees to avoid conflicts of interest and to ensure legitimacy.[206] In recent analyses, the experts criticize the dominance of executive-led and institutional models of intelligence oversight, particularly those grounded in liberal democratic traditions that emphasize secrecy, professional expertise, and trust-based relations between intelligence agencies and their formal overseers (e.g. executive-appointed committees or ministries). It argues that such models often exclude civil society and suppress more agonistic or participatory forms of democratic engagement, such as whistleblowing, litigation, and activism.[207] Barker and Petrie have analysed

203 Born, H. and Leigh, I., 2005. *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*. Oslo: Publishing House of the Parliament of Norway.

204 Leigh, I., 2007. 'The accountability'.

205 Rascoff, S.J., 2016. 'Presidential Intelligence'. *Harvard Law Review*, 129/3, 633–676. Available at: https://harvardlawreview.org/2016/01/presidential-intelligence/ [Accessed 5 November 2025]

206 Raab, C.D., 2017. 'Security, privacy and oversight'. In: E. Sutherland, K. Brown and A. Mackenzie, eds. *Security in a Small Nation: Scotland, Democracy, Politics*. Cambridge: Open Book Publishers, 103–124.

207 Kniep, R., Ewert, L., Léon Reyes, B., Tréguer, F., Mc Cluskey, E. and Aradau, C., 2024. *Towards democratic intelligence oversight: Limits, practices, struggles*. Review of International Studies, 50/1, 209–229.

the conduct of oversight in relation to the intelligence communities of the Five Eye Nations and concluded that what might work well in one country may not necessarily be consistent with the institutions and norms of another. Instead, the oversight frameworks reflect each nation's political structure, history, and culture, and therefore differ in some of the particulars. However, each country has developed a framework that includes a system of checks and balances that spans the various branches of government, and which aims to ensure that agencies are accountable for both their administration and expenditure and the legality and propriety of their activities.[208] Andrew Defty in his research has examined the role of the executive in the oversight of the UK intelligence and security agencies. It traces the evolution of ministerial accountability for the UK intelligence and security agencies. It also raises questions about the capacity of ministers to provide effective scrutiny in this area, focusing on ministers' knowledge and understanding of intelligence, ministerial workload and potential conflicts of interest.[209] Mark Phythian assessed the British experience with intelligence accountability through an analysis of the principal mechanism that exists to provide for it – the parliamentary Intelligence and Security Committee.[210] Keiran Hardy and George Williams have provided a detailed analysis of Australia's executive oversight mechanisms for its six intelligence agencies, emphasizing the challenges posed by secrecy and limited parliamentary or judicial scrutiny. The authors highlight the central role of executive-appointed statutory bodies, such as the Inspector General of Intelligence and Security and the Independent National Security Legislation Monitor, in authorizing, reviewing, and evaluating intelligence activities. While these mechanisms benefit from access to classified information and strong investigative powers, their effectiveness is constrained by their largely recommendatory nature and reliance on government willingness to implement reforms. The study concludes that Australia has a wide array of oversight tools. However, it is pointed out, significant vulnerabilities remain, particularly when executive bodies oversee agencies within the same branch of government.[211] The article *Executive and Legislative Oversight of the Intelligence System in Argentina* by Eduardo E. Estévez outlines the evolution of democratic oversight mechanisms in Argentina's intelligence sector. While significant reforms culminated in the passage of the 2001 National Intelligence Law, gaps remain, particularly in executive-level oversight, public complaints mechanisms, and the regulation of certain intrusive methods.

208 Barker, C. and Petrie, C., 2017. *Oversight of Intelligence Agencies: A Comparison of the 'Five Eyes' Nations*. Parliamentary Library Research Paper Series 2017–18, Australia: Parliament of Australia. Available at: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1718/IntelligenceOversight [Accessed 1 May 2025].

209 Defty, A., 2021. "Familiar but not intimate': executive oversight of the UK intelligence and security agencies.' *Intelligence and National Security*, 37/1, 57–72.

210 Phythian, M., 2007. 'The British experience with intelligence accountability.' *Intelligence and National Security*, 22/1, 75–99.

211 Hardy, K. and Williams, G., 2016. 'Executive oversight of intelligence agencies in Australia.' In: Z.K. Goldman and S.J. Rascoff, eds. *Global intelligence oversight: Governing security in the twenty-first century*. New York: Oxford University Press, 315–334.

The article highlights that while legal structures exist, the effectiveness of oversight depends on the political will of both the legislature and the executive.[212]

The article tends to conclude that while executive oversight is indispensable, it should not be dominant. It must function in a complementary role reinforcing, rather than replacing, parliamentary, judicial, and civic forms of intelligence accountability.

2.3.2. Institutions responsible for executive oversight and the core elements of their oversight functions

In modern states the security and intelligence agencies have a vital role to play serving and supporting government in its domestic, defence and foreign policy by supplying and analysing relevant intelligence and countering specified threats.[213]

At the same time, the agencies continue to be accountable to the executive branch. The executive branch's oversight of intelligence services is typically institutionalized through various governmental bodies and structures, including ministries (usually defence or interior), national security advisory structures, and, in presidential systems, the office of the president or head of state. This framework ensures that intelligence activities align with national security policies and legal standards. For instance, in many NATO countries, authorities such as special central governmental structures, ministries of defence, foreign affairs, and interior, along with other relevant agencies, have specific security or intelligence responsibilities, facilitating coordinated oversight and policy implementation.[214] Key components of executive oversight include ministerial responsibility for guiding and supervising intelligence services, ensuring that their activities align with national policy and legal frameworks. It also involves control over covert actions (in countries where they are used), which often require direct approval from ministers or heads of state due to their sensitive nature. Additionally, the executive oversees international cooperation, particularly in matters of intelligence sharing and foreign operations, where state accountability and diplomatic considerations are crucial. Finally, internal checks such as the work of inspectors general and internal audit bodies play an important role in preventing the misuse of intelligence powers and guarding against political abuse within the executive branch.[215] The executive branch can

212 Estévez, E.E., 2005. 'Executive and legislative oversight of the intelligence system in Argentina.' In: H. Born, L.K. Johnson and I. Leigh, eds. *Who's Watching the Spies? Establishing Intelligence Service Accountability*. Washington, D.C.: Potomac Books, 160–179

213 Leigh, I., 2007. 'The accountability'.

214 Vitkauskas, D., 1999. *The Role of a Security Intelligence Service in a Democracy*. [online] NATO Democratic Institutions Fellowships Programme. Available at: https://www.nato.int/acad/fellow/97-99/vitkauskas.pdf [Accessed 1 May 2025]

215 Born, H. and Leigh, I., 2005. *Making Intelligence Accountable*.

be involved in up to seven key areas of intelligence oversight, depending on the country's legal and political system. These areas reflect the range of responsibilities typically undertaken by executive offices to ensure effective, lawful, and accountable intelligence governance.

1. **Budgetary oversight:** Executives may play a role in approving and allocating intelligence budgets prior to submitting it to the legislators.

2. **Leadership appointments:** Executives may play a role in selecting, appointing, or dismissing intelligence service leaders as a means of exercising oversight and ensuring institutional accountability.

3. **Strategic tasking and priority setting:** Executives may define national intelligence priorities through directives or strategic policy documents, shaping the service's focus and guiding its medium and long-term goals.

4. **Operational authorization:** Executives may grant or deny approval for high-risk or politically sensitive operations, particularly those leading to potential diplomatic crises or legal uncertainties.

5. **Legal and policy framework development:** executives may propose or support amendments to legislation and regulations governing intelligence, ensuring the legal basis remains responsive and able to cope with new security challenges.

6. **Compliance and accountability mechanisms:** by using audits, reports, reviews of activities, and other internal means, executives ensure that the service complies with protocols.

7. **Crisis command and emergency powers:** during the crisis or emergency, executives may gain direct access to the operational control of the service and activate their emergency powers.

It is evident that the powers of the executive branch vary depending on a country's political system and constitutional framework, making it challenging to generalize their oversight functions. The table below presents a broad overview of three key institutions and the oversight functions they are most likely to hold, as discussed below.

Executive branch	Budgetary oversight	Leadership appointments	Strategic tasking/ priority setting	Operational authorization	Compliance with laws	Crisis command
Ministries	✔	✔	✔	✔	✔	✔
National security advisory			✔	✔	✔	
Office of president or prime minister	✔	✔	✔	✔	✔	

2.3.2.1. Ministries

In many NATO countries, ministries have traditionally overseen intelligence agencies and are involved across all seven core areas of executive oversight. While the extent of their role varies depending on the national context, political system and legal framework, ministries generally hold the most substantial responsibility for intelligence oversight within the executive branch. Ministers need access to relevant information in the hands of the agency or to assessments based upon it through intelligence assessments and, they must also be able to give a public account where necessary about the actions of the security sector. Conversely, officials need to be able to brief government ministers on matters of extreme sensitivity.[216]

They play a key role in the appointment and dismissal of intelligence service leadership. This does not imply involvement in day-to-day human resource management, but often includes the authority to nominate or formally appoint agency heads. For instance, the Head of the Federal Office for the Protection of the Constitution (BfV), the domestic intelligence service in Germany, is appointed by the Federal Minister of the Interior, with approval from the federal cabinet.[217] The Minister also has the authority to dismiss the head of BfV.

216 Leigh, I., 2007. 'The accountability'.

217 ZEIT ONLINE, 2018. 'Hintergrund: Wer ernennt und entlässt den Verfassungsschutz-Chef?' [online] 12 September. Available at: https://www.zeit.de/news/2018-09/12/wer-ernennt-und-entlaesst-den-verfassungsschutz-chef-180912-99-930246. [Accessed 1 May 2025]. Interestingly the Federal Act on the Protection of the Constitution outlines the responsibilities and oversight of the BfV, it does not specify the appointment procedures for its leadership.

Ministries have certain powers in the area of budgetary oversight of intelligence service. They can be engaged in approving, allocating and reviewing budget, especially prior to approval at the parliament. For instance, the Federal Ministry of the Interior of Germany is responsible for managing the budget of the BfV by reviewing and consolidating budget proposals before they are submitted to the Bundestag for final approval.[218] In Norway, the Ministry of Defence prepares the budget request for the intelligence service as part of the national defence budget, which is then submitted to Parliament for approval.[219]

Ministries are actively involved in setting priorities and defining strategic taskings for intelligence services. The emphasis here is on the term *strategic*, as it is neither appropriate nor desirable for the executive to interfere in the day-to-day operations of intelligence agencies. Their role is to help shape long-term priorities and guide the strategic direction of intelligence activities. For instance, in the Netherlands, the Council for Security and Intelligence (RVI) establishes the 'Integrated Instruction for the Intelligence and Security Services' (GA) once every four years. The GA is a secret document for the MIVD and the General Intelligence and Security Service (AIVD). It states what the services must investigate in the coming four years, which goals must be achieved and which investigations have priority. The RVI consists of the Ministers of the Interior and Kingdom Relations, Defence, Foreign Affairs and Security and Justice. The Prime Minister is the chairman.[220]

218 German Bundestag, n.d. *Adoption of the federal budget*. [online] Available at: https://www.bundestag.de/en/parliament/adoption-245712 [Accessed 1 May 2025].

219 The law does not specify the procedures but the Ministry exercises management and control via CHOD. Norwegian Ministry of Defence, 2021. *Act relating to the Norwegian Intelligence Service*. [online] Oslo: EOS Committee. Available at: https://eos-utvalget.no/wp-content/uploads/2021/06/Official-translation-of-the-Act-relating-to-the-Norwegian-intelligence-service.pdf [Accessed 1 May 2025]

220 Ministerie van Defensie, n.d. *De overheid bepaalt wat de MIVD doet*. [online] Available at: https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/overheid-als-opdrachtgever [Accessed 1 May 2025].

The Case of Canada

The Minister of Public Safety and Emergency Preparedness and the Minister of National Defence have important responsibilities with regard to the national security and intelligence agencies in their respective portfolios.

The Minister of Public Safety and Emergency Preparedness is responsible for three national security agencies: the Canada Border Services Agency (CBSA), CSIS and the Royal Canadian Mounted Police (RCMP). The Minister is also responsible for Public Safety Canada. The Minister of National Defence is responsible for the Communications Security Establishment (CSE), the Department of National Defence (DND) and the Canadian Armed Forces (CAF).

Ministers can issue formal directions that establish guidelines on the conduct and management of operations, though the principle of police independence limits direct ministerial involvement in day-to-day law enforcement operations. Ministerial Directions (MDs) may also specify reporting requirements and procedures for obtaining approval for agency activities.

A number of MDs are currently in effect for the CBSA, CSE, CSIS and the RCMP. For example, in 2015, CSIS was issued wide-ranging new MD on operations and accountability. The RCMP is also subject to several MDs that provide guidance on aspects of national security investigations related to sensitive sectors, accountability, and cooperation. MDs on information sharing with foreign entities have also been issued to the CBSA, CSE, CSIS and the RCMP. These MDs established a consistent process for deciding whether to share information with foreign entities where there may be a risk of mistreatment stemming from the sharing of information, in accordance with Canada's laws and legal obligations.[221]

221 Public Safety Canada, 2016. *Our Security, Our Rights: National Security Green Paper, 2016 – Background Document*. Available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/index-en.aspx [Accessed 1 May 2025].

It is worth noting that ministries are involved in granting or denying approval for specific intelligence operations that carry significant legal, political, or diplomatic implications. This may include covert actions, high-risk engagements, or cross-border operations requiring executive-level authorization. According to the Section 16 of the Canadian Security Intelligence Service Act, the Service may, in relation to the defence of Canada or the conduct of the international affairs of Canada, assist the Minister of National Defence or the Minister of Foreign Affairs, within Canada, in the collection of information or intelligence relating to the capabilities (…) The assistance provided under subsection (1) may include the collection, from within Canada, of information or intelligence that is located outside Canada if the assistance is directed at a person or thing in Canada or at an individual who was in Canada and is temporarily outside Canada. (…) The Service shall not perform its duties and functions under subsection (1) unless it does so on the personal request in writing of the Minister of National Defence or the Minister of Foreign Affairs; and with the personal consent in writing of the Minister.[222] In Norway, the intelligence service is obliged to submit as matters for the decision of Minister: any agreements for establishing collaboration with foreign services; launching a special operation that may have political implications; and other cases of particular importance.[223] In the UK, under the Investigatory Powers Act 2016, intelligence agencies must obtain a warrant signed by the Secretary of State (typically the Home Secretary or Foreign Secretary) for intrusive activities such as the interception of communications, equipment interference, or covert human intelligence operations.[224]

The executive branch plays a role in proposing or endorsing amendments to laws and regulations governing intelligence activities. For instance, in April 2025, Lithuania's Ministry of Defence formally registered proposed amendments to the Intelligence Service Law.[225] If Parliament approves the amendments, certain surveillance-related actions could be initiated on the basis of a decision by the head of an intelligence institution, without having to wait for a court ruling.

222 Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23. [online] Available at: https://laws-lois.justice.gc.ca/eng/acts/c-23/FullText.html [Accessed 1 May 2025].

223 Norwegian Ministry of Defence, 2021. *Act relating to the Norwegian Intelligence Service*.

224 Investigatory Powers Act 2016, Part 2, UK Public General Acts 2016 c.25. Available at: https://www.legislation.gov.uk/ukpga/2016/25/part/2. [Accessed 5 November 2025]

225 Bieliavska, J., 2025. 'Žvalgybai siūloma suteikti daugiau įgaliojimų'. *ELTA*, 6 April 2025.

Lithuania's MoD Proposal in 2025

1. Such actions could include, for example, entering a residence or other premises, accessing vehicles, intercepting electronically transmitted communications or messages, seizing documents or objects, and monitoring financial operations. However, these actions would only be permitted when 'urgent measures are necessary to prevent threats to the national security of the Republic of Lithuania.' According to the MoD, intelligence operations must be conducted swiftly, and response time is critical. The drafters of the proposal argue that failing to act immediately may result in the loss of critically important information that cannot be recovered later.

2. Importantly, after initiating urgent surveillance actions, the head of the intelligence institution must apply to a regional court within 24 hours for judicial authorization *via* a reasoned court order.

3. The registered amendments also propose allowing intelligence agencies to check the identity documents of individuals posing a threat to national security, as well as vehicle, cargo, and weapons documents. Temporary seizure of such items for inspection would be allowed, but only if there is data indicating that the person poses a risk or threat to national security and if the aim is to prevent such risks.

4. The amendments also provide individuals who believe their rights have been unjustly violated with the option to defend them not only in court but also by submitting a complaint to the intelligence ombudsman.

5. The amendments also foresee the possibility of intelligence agencies covertly collecting individuals' fingerprints, voice samples, scent traces, and other samples. This provision is especially relevant for verifying identity, particularly when there is evidence that a person may be using cover identities. To support object identification, it is proposed that intelligence services be allowed to use any type of marking substances or methods that do not pose a danger to human life or health.

6. The amendments prohibit the use of simulated criminal activity if it would pose a direct threat to human life or health or could cause other serious consequences. It also prohibits provoking a person to commit an offense.

One of the most complex and rarely exercised aspects of executive oversight involves the direct operational control of intelligence services. In exceptional circumstances, such as emergencies or crises, ministries may take on an expanded role by activating emergency powers. In certain cases, it might seem that they are assuming limited control or coordination over specific intelligence operations. Canadian legislation embodies the principle in the Canadian Security Intelligence Service Act 1984, referring to the director of the service having 'the control and management of the Service' that is 'under the direction' of the Minister.[226]

The Case of France[227]

France declared a state of emergency on the evening of the November 13, 2015 after the deadliest terror attacks on French soil in modern history left 130 people dead in the Paris region. The government pushed through fresh anti-terror laws, granting police and intelligence agencies extended powers, as the country faced a wave of further attacks in French cities and towns, such as Nice, St-Étienne-du-Rouvray, Villejuif and Rambouillet. The state of emergency expired in November 2017, when President Emmanuel Macron replaced it with a tough anti-terror law. The new law permanently legalised several aspects of the state of emergency such as extended police powers to search homes, restrict movement or close radical religious sites (HRW report). Nevertheless, police did not conduct intelligence operations *per se*.

However, the main intelligence service responsible for counterterrorism is the DGSI (General Directorate for Internal Security), which operates under the authority of the Ministry of the Interior. This structure might imply that, in 2015, the French Ministry of the Interior—through the DGSI—held operational control over intelligence activities targeting terrorist threats on French territory. However, coordination with other intelligence services also occurred at the presidential level, under the supervision of the National Intelligence Advisor. In 2017, this role evolved into the National Coordinator for Intelligence and Counterterrorism (CNRLT), a body that reports directly to the Élysée Palace (interview with French intelligence expert).

Following the failed coup attempt in July 2016, the Turkish government declared a state of emergency and issued several emergency decree laws that significantly expanded the powers of the executive branch, particularly the security ministries.[228] The National Intelligence Organization (MIT) had previously reported to the

226 Leigh, I., 2007. 'The accountability'.

227 Human Rights Watch, 2015. *France: State of Emergency Declared After Paris Attacks*, 19 November.

228 Venice Commission, 2016. *Opinion on Emergency Decree Laws Nos. 667–676 Adopted Following the Failed Coup of 15 July 2016*. European Commission for Democracy through Law (Venice Commission), Council of Europe. Available at: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)037-e [Accessed 5 May 2025].

Prime Minister, but in a decree issued under emergency powers introduced following the defeated coup, it was announced that it would now answer to the president.[229] While there is no proof of this, the MIT's coordination and possibly some aspects of control fell under the security Ministries in the immediate post-crisis period.

2.3.2.2. National security Advisory Bodies

National security advisors (NSAs) play an important role in executive oversight in NATO countries. While their role might be seen as being largely limited to advising, coordinating, and helping with priority-setting for intelligence service, some NATO countries have patterned their NSAs directly along the lines of the U.S. model.[230] Their role is visible in priority setting, legal and policy development and compliance and accountability. They play an important role in translating intelligence input into policy. In other words, advisors often do not have direct authority over agencies. Rather, they serve as a bridge between intelligence service outputs to national security strategy priorities. For instance, in the UK, the NSA was responsible for the line management of the heads of the intelligence agencies – MI5, MI6 and GCHQ. Given Jonathan Powell's (current NSA) status as a political special adviser, these agencies report to the cabinet secretary: though Powell will continue to work closely with them so he can best advise the Prime Minister. The NSA must also build close international relationships with allies. This is especially important with the international counterparts of the members of the Five Eyes intelligence sharing agreement (which the UK is part of alongside the US, Canada, Australia and New Zealand) and other members of the G7.[231] In the United States, the NSA's responsibilities include integrating intelligence assessments into policy decisions and aligning intelligence priorities with the administration's objectives. According to the National Intelligence Priorities Framework, the President and the National Security Advisor determine the top-tier national intelligence priorities, ensuring that intelligence efforts are responsive to the nation's strategic needs.[232] In Croatia, the National Security Advisor to the President of the Republic plays a significant role within the country's security and intelligence framework. The advisor is a member of the National Security Council, the central coordinating body responsible

229 *Daily Sabah*, 2017. 'Turkey's intel agency MİT to report to president with new decree.' *Daily Sabah*, 26 August. Available at: https://www.dailysabah.com/turkey/2017/08/26/turkeys-intel-agency-mit-to-report-to-president-with-new-decree [Accessed 5 May 2025].

230 Inderfurth, K.F. & Johnson, L.K., 2004. *Fateful decisions: inside the National Security Council*. New York: Oxford University Press.

231 Given his status as a special adviser, Powell will need to attend the National Security Council, rather than be its secretary, as his predecessors have done. He will report to the Prime Minister, while the heads of the intelligence agencies and deputy NSAs will need to report directly to the cabinet secretary. Institute for Government, 2020. *National security adviser*. [online] Available at: https://www.instituteforgovernment.org.uk/explainer/national-security-adviser [Accessed 5 May 2025].

232 Office of the Director of National Intelligence (ODNI), 2020. *Intelligence Community Directive 204: National Intelligence Priorities Framework*. [online] Available at: https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf [Accessed 5 May 2025].

for assessing security threats, formulating guidelines, and making decisions to safeguard national security interests.[233]

NSAs often coordinate cross-government input into national security legislation and advise the executive on legal reforms related to intelligence. National security advisory bodies often review intelligence performance, coordinate interagency evaluations, and present findings to top leadership. In Canada, the National Security and Intelligence Advisor supports oversight coordination and ensures intelligence complies with national policy through their reports to the Prime Minister.[234]

Mandate Letter of the National Security and Intelligence Advisor (Canada)[235]

'Your role as my principal advisor on national security and intelligence is critical to achieving the objectives of a better understanding, managing, and responding to threats. Public discussions on foreign interference reaffirm the need for a stronger, more clearly articulated NSIA position that can oversee and guide the intelligence process from collection and assessment, through policy development, to our response and operational coordination. It is a dynamic, ever-changing, and evolving role depending on current affairs and priorities. Enhancing your role will help ensure the right information and intelligence gets to the right people at the right time, and that decision makers are given actionable options and advice. At the same time, we need to improve transparency and dialogue with Canadians, especially those directly impacted by emerging threats, to help raise awareness and enhance our collective ability to respond. This includes better dialogue with Parliamentarians, civil society representatives, diaspora communities, provinces and territories, Indigenous groups, allied partners, industry, and other Canadians. As my National Security and Intelligence Adviser, I expect you to manage the flow of intelligence and analysis necessary for me to effectively fulfil my duties as Prime Minister. In deciding what intelligence and analysis should reach me, as Prime Minister, please take into account Canada's strategic priorities, urgent issues, and relevant advice from the Clerk of the Privy Council, Ministers, Deputy Ministers and other senior officials in Canada's national security apparatus.'

233 Office of the National Security Council, n.d. *National Security Council*. [online] Available at: https://www.uvns.hr/en/about-us/glossary/national-security-council [Accessed 5 May 2025].

234 Privy Council Office, 2024. *Mandate Letter of the National Security and Intelligence Advisor*. [online] Available at: https://www.canada.ca/en/privy-council/corporate/clerk/role/mandate-letter-national-security-intelligence-advisor.html [Accessed 5 May 2025].

235 Privy Council Office, 2024. *Mandate Letter of the National Security and Intelligence Advisor*. [online] Available at: https://www.canada.ca/en/privy-council/corporate/clerk/role/mandate-letter-national-security-intelligence-advisor.html. [Accessed 5 November 2025]

2.3.2.3. Presidential Bodies and Prime Ministerial Offices

In presidential or semi-presidential systems, intelligence services may be directly accountable to the president or their office. In Turkey, intelligence services, such as MIT, are directly subordinated to the presidency, reflecting a highly centralized model.[236] In Poland, the President's influence over the security services is primarily exercised through the National Security Bureau, which is responsible for implementing presidential directives on national security matters and offering administrative support to the National Security Council.[237] The Prime Minister, on the other hand, holds formal supervisory powers over the nation's security and intelligence agencies. There is the position of the Minister-Coordinator of Special Services. However, his appointment is optional for any Prime Minister. The relevant minister, a minister without portfolio (or recently just undersecretary of state), does not have independent powers or an institutional place of their own in the government structures. Their actual importance strongly depends on the support of the Prime Minister.[238]

NSAs play a significant role across all key areas of oversight, excluding direct operational control. However, the extent and nature of their oversight responsibilities are shaped by the involvement and authority of other actors, particularly parliaments. Broadly speaking, presidential administrations or prime ministers' offices are especially influential in the appointment of intelligence leadership, authorization of special operations, and definition of strategic priorities.

In the UK, the Prime Minister has ultimate authority over the appointment of the heads of MI5, MI6 (Secret Intelligence Service), and GCHQ. Of course, these appointments are coordinated with the Cabinet Office and Foreign, Commonwealth & Development Office (FCDO). For instance, the Foreign Secretary, with the agreement of the Prime Minister, approved the appointment of Richard Moore CMG as the new Chief of the Secret Intelligence Service (MI6) in 2020.[239] The President in France plays a central role in the appointment of the heads of French intelligence agencies, such as the DGSE (external intelligence) and DGSI (internal security). These appointments are made upon proposals from the Prime Minister and relevant ministers (Interior, MoD), and typically formalized by decree from the Élysée Palace.[240] For instance, the appointment of Nicolas Lerner as Director-General of the DGSE was formalized by a presidential decree 20 December, 2023. This decree

236 *Daily Sabah*, 2017. 'Turkey's intel agency'.

237 National Security Bureau. [online] Available at: https://en.bbn.gov.pl/en/national-security-coun/99,The-National-Security-Council.html [Accessed 5 May 2025].

238 Gogolewska, A., 2021. 'Transformation of State Security and Intelligence Services in Poland – A Job Still Unfinished.' *Connections: The Quarterly Journal*, 20(1), 9–32. Available at: https://connections-qj.org/article/transformation-state-security-and-intelligence-services-poland-job-still-unfinished. [Accessed 5 May 2025].

239 Foreign & Commonwealth Office and The Rt Hon Dominic Raab, 2020. *Appointment of the new Chief of the Secret Intelligence Service (MI6)*. [online] GOV.UK. Available at: https://www.gov.uk/government/news/appointment-of-the-new-chief-of-the-secret-intelligence-service-mi6--2 [Accessed 5 May 2025].

240 France. 2023. *Décret du 20 décembre 2023 portant nomination du directeur général de la sécurité extérieure*. [online] *Journal officiel de la République française*. Available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000048621922 [Accessed 18 May 2025].

was issued by President Emmanuel Macron and countersigned by Prime Minister Élisabeth Borne and Minister of the Armed Forces Sébastien Lecornu.[241]

Furthermore, the presidential and prime minister bodies are involved in intelligence tasking as this is the responsibility of the executive branch of government and reflects a state's foreign, security, and defence policies. The output of the tasking process, commonly referred to as a 'statement of intelligence priorities', is usually summarized in a document that is approved by government ministers or the head of the executive.[242] This document defines the priorities for the collection and processing of intelligence by a state's intelligence agencies, three national examples of which are shown in the table below.

Country	Canada	UK	USA
Title of document	*Government Intelligence Priorities*	*Intelligence Coverage and Effects Plan (ICE)*	*National Intelligence Priorities Framework (NIPF)*[243]
Responsible state organ(s)	Set by the Cabinet Committee on Intelligence and Emergency Management – chaired by the Prime Minister.	Drafted by the National Security Secretariat and approved by the National Security Council – chaired by the Prime Minister.	Set by the Office of the Director of National Intelligence. Reviewed by the National Security Council and approved by the President.
Content of document	Thematic priorities on basis of domestic and international threats.	Thematic and geographic priorities.	Thematic priorities which are linked to countries and non-state actors.
Review process	Strategic Intelligence Requirements reviewed every six months with new priorities process every two years.	Reviewed annually but with scope for 'in year changes'.	Reviewed every six months.

241 *Le Monde* with AFP, 2023. 'French domestic intelligence chief appointed head of foreign espionage.' *Le Monde*, 20 December. Available at: https://www.lemonde.fr/en/france/article/2023/12/20/french-domestic-intelligence-chief-appointed-head-of-foreign-espionage_6360939_7.html [Accessed 18 May 2025].

242 Geneva Centre for Security Sector Governance. 2021. *The Role of Parliaments in Overseeing Intelligence Tasking*. [online] Geneva: DCAF. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/ThematicBrief_StrategicTasking2021.pdf. [Accessed 5 November 2025]

243 For the USA, the NIPF document is really a broad 'umbrella' guideline. Priorities are set more specifically in specialized and more narrowly focused documents. Comments received from L.Johnson

Geneva Centre for Security Sector Governance. 2021. *The Role of Parliaments in Overseeing Intelligence Tasking*. [online] Geneva: DCAF. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/ThematicBrief_StrategicTasking2021.pdf.

These bodies play an important role in authorizing special operations. In the US, the President must personally authorize all covert operations conducted by the CIA or other intelligence agencies, under Title 50 of the U.S. Code. This is done through a Presidential Finding, which must be reported to congressional intelligence committees.[244] In 2020, the Pentagon confirmed the strike killing Soleimani, who as head of the Islamic Revolutionary Guards Corps (IRGC) Quds Force had been the architect of Teheran's proxy conflicts in the Middle East. US President Donald Trump said that he ordered a precision strike to 'terminate' a top Iranian commander who was plotting 'imminent and sinister attacks' on Americans, adding that the decision was one of deterrence rather than aggression.[245] L. Johnson discusses the Soleimani strike as a high-stakes covert action that blurred the lines between covert and overt military operations. He emphasizes the ethical and legal complexities of such actions, particularly concerning international law and the norms governing state conduct. In his analysis, he argues that while covert operations can be necessary tools of foreign policy, they must be conducted within a framework that ensures maximum possible transparency and adherence to democratic principles[246].

In times of crisis or emergencies, these bodies, while tempting to see, may assume enhanced control or coordination over intelligence services, but they do not take direct operational control in a literal sense (i.e., issuing tactical orders to intelligence operatives). Instead, their role typically involves centralizing decision-making, approving exceptional measures, directing coordination between intelligence and other security institutions. A compelling example of the executive's role is connected to the UK's involvement in Iraq. Ahead of the war in that country, Prime Minister Tony Blair's office faced allegations of pressuring the Joint Intelligence Committee to exaggerate intelligence regarding Saddam Hussein's weapons capabilities. The Hutton Inquiry and Butler Review later investigated the extent of this executive influence.[247] This indicates an attempt of penetration into the intelligence cycle allowing political agendas or pressures to influence how intelligence is collected, interpreted, or presented.

244 Legal Information Institute (LII), 2025. *50 U.S. Code § 3093 – Presidential approval and reporting of covert actions*. [online] Cornell Law School. Available at: https://www.law.cornell.edu/uscode/text/50/3093 [Accessed 18 May 2025].

245 CNN, 2020. *Multiple rockets hit near Baghdad airport, killing Iranian commander Qasem Soleimani*. [online] 3 January. Available at: https://edition.cnn.com/2020/01/02/middleeast/baghdad-airport-rockets/index.html [Accessed 18 May 2025].

246 Johnson, L.K., 2022. *The Third Option: Covert Action and American Foreign Policy*. Oxford: Oxford University Press.

247 Clark, D., 2004. 'Blair sexed up the evidence to justify his own decision.' *The Guardian*, 13 July. Available at: https://www.theguardian.com/politics/2004/jul/13/butler.iraq [Accessed 18 May 2025].

2.3.3. Challenges of executive oversight

The very nature of intelligence work rooted in secrecy and complexity presents serious challenges to effective oversight. Executives entitled with this responsibility must find appropriate ways to conduct oversight and make intelligence systems accountable while not penetrating into their daily operations and respecting operational confidentiality. There are four key challenges that deserve the attention here.

2.3.3.1. Politicisation, accountability and managerial control

The first set of issues is linked to the risk of politicisation, where political masters might capitalize on their oversight competences and ask the intelligence service to serve their political interests. As L. Johnson mentioned, an important concern for overseers is the question of intelligence politicization: 'cooking' information to suit the political needs and ideological inclinations of policymakers. The Church Committee recorded instances of politicization and, from time to time, new charges arise. In 2002, Department of Defense officials complained that CIA intelligence on Iraq failed to match their expectations, and they established a new intelligence unit of their own (the Office of Special Plans). This was perhaps to bypass the intelligence community and produce information that better reinforced the administration's plans to invade Iraq and the preconceived views on Iraq held by Pentagon officials.[248] Another notable example is highlighted in *America's Secret Power: The CIA in a Democratic Society*, by Johnson who examines the Huston Plan as a significant example of the misuse of intelligence powers within the United States. The Huston Plan, written in 1970, proposed a series of covert operations aimed at intensifying surveillance and infiltration of domestic dissenters, including anti-war activists and civil rights groups. Johnson discusses how the plan was initially approved by President Nixon but faced opposition from FBI Director J. Edgar Hoover, leading to its formal rescission.[249]

Such actions can blur the line between national security and political agendas, weakening independence of oversight structures. There might be the temptation of the executive to put political appointees in senior positions in the services. These people lack experience and could drive an agenda to only working towards what the executive wants to hear rather than objective truths. It also breaks trust with international partners who might not wish to share information. This is based on the fact that they will lose control of information to a service and regime with particular objectives that they do not agree with.[250] Furthermore, there might

248 Johnson, L.K., 2011. 'Intelligence accountability in the United States'. In: H. Born, L.K. Johnson, I. Leigh and A. Wills, eds. *Who's watching the spies? Establishing intelligence service accountability*. Washington, D.C.: Potomac Books, 64.

249 Johnson, L.K., 1989. *America's secret power: the CIA in a democratic society*. New York: Oxford University Press.

250 Email received from senior intelligence expert David Watson, 20 April 2025.

be the use of the services to gather intelligence or take action against political opponents. As the executive sets the requirements, it would be easy to use this to gather intelligence on political opponents. Again, this can happen in developed democracies. Whilst there is no evidence that the CIA had participated directly in Watergate, there is enough evidence to suggest that the individuals involved were using skills and equipment supplied by the CIA. Most were former CIA employees or sources. There are multiple examples in other 'democratic' countries where the executive has used the services to spy on political opponents, e.g. Serbia.[251] A report found that Serbia's intelligence agency installed spyware on the phones of journalists and activists.[252]

When intelligence agencies are influenced by political agendas, their ability to operate independently is compromised and consequently, the level of accountability is reduced. For example, the Zondo Commission, officially known as the Judicial Commission of Inquiry into Allegations of State Capture, Corruption and Fraud in the Public Sector including Organs of State. The Commission was established in 2018 in South Africa and was tasked with investigating allegations of widespread corruption and abuse of power under the administration of former President Jacob Zuma, including the politicisation and dysfunction of key intelligence institutions such as the State Security Agency (SSA).[253] The commission highlighted several factors that contributed to the abuse within the SSA, such as merger of the National Intelligence Agency (NIA) and the South African Secret Service (SASS) into the SSA. This merger, done *via* a presidential proclamation rather than legislation, left the agency operating without a clear legal basis until 2013. The highly centralized structure of the SSA made it easier for a corrupt director-general to misuse power. Additionally, the agency's focus shifted to protecting the state and the president rather than ensuring public security, fostering space for abuse. Oversight bodies, including the Joint Standing Committee on Intelligence, the Inspector General, and the Auditor General, failed to adequately monitor the agency, leaving oversight weak or non-existent.[254] On the other hand, there can be a power imbalance between the executive and the services if the executive is dependent on the services for most of their information on a particular subject. For example, the level of threat by a terrorist group is driven by the information from the services. The executive cannot make an independent assessment. This leaves it open for services to exaggerate the threat in order to obtain more resources.[255]

251 Email received from senior intelligence expert David Watson, 20 April 2025.

252 *Deutsche Welle*. (2024). 'Serbia monitors journalists and dissidents with spyware.' [online] Available at: https://www.dw.com/en/serbia-monitors-journalists-and-dissidents-with-spyware/a-71132881. [Accessed 18 May 2025].

253 State Capture Commission (2022) *Judicial Commission of Inquiry into Allegations of State Capture, Corruption and Fraud in the Public Sector including Organs of State*. Available at: https://www.statecapture.org.za/. [Accessed 18 May 2025].

254 Zwakala, M. (2022) 'Zondo commission's report on South Africa's intelligence agency is important, but flawed', *The Conversation*, 28 July. Available at: https://theconversation.com/zondo-commissions-report-on-south-africas-intelligence-agency-is-important-but-flawed-186582. [Accessed 18 May 2025].

255 Email received from senior intelligence expert David Watson, 20 April 2025.

There are also commonsense reasons for a formal separation between executive oversight and managerial control of the agencies and their operations.[256] As has been mentioned, the executive branch is actively involved in setting priorities and defining strategic taskings for intelligence services. However, it is crucially important to avoid their engagement in managerial control of the agencies and their operations and rather concentrate on strategic tasking to guide the intelligence agencies. Finally, there has to be a high degree of trust coupled with checks and balances between the executive and the services. By their very nature, operations are covert. This means that it is difficult to share details of operations and there has to be a strict need to know basis. The executive has to trust and verify that the services are telling them the truth.

2.3.3.2. Coordination and jurisdictional overlap

The second challenge in executive oversight lies in the coordination (or lack thereof) with other oversight actors such as parliament, the judiciary, and civil society. While executive bodies hold primary responsibility for directing and scrutinising intelligence activities, effective oversight often requires collaboration with other institutions to ensure a comprehensive system of checks and balances. However, coordination is frequently hindered by institutional silos, differing mandates, and limited information-sharing protocols.

For example, the UK's experience, as highlighted in the *Big Brother Watch and Others v. United Kingdom* judgment by the European Court of Human Rights (ECtHR), illustrates the challenges posed by weak coordination between oversight bodies in the intelligence sector. This case arose in response to the revelations by Edward Snowden in 2013, which exposed large-scale surveillance practices by the UK's intelligence agencies, particularly the Government Communications Headquarters (GCHQ). The applicants, including journalists, human rights organizations, and privacy advocates, argued that the UK's surveillance programs violated their rights under the European Convention on Human Rights (ECHR), specifically article 8 (right to respect for private and family life) and article 10 (freedom of expression).[257] The Court held that bulk interception of communications is not inherently contrary to the ECHR. However, it ruled that the UK's specific implementation of such a regime breached both the right to privacy and the freedom of expression. The Court identified serious shortcomings in the system, particularly the absence of independent oversight through key stages, such as the selection of communication channels for surveillance; the criteria and search terms used to filter data; and the process by which analysts reviewed intercepted content. Furthermore, the Court found that the framework for acquiring communications

256 Email received from senior intelligence expert David Watson, 20 April 2025.

257 European Court of Human Rights, 2021. *Big Brother Watch and Others v. the United Kingdom*, Applications nos. 58170/13, 62322/14 and 24960/15, Grand Chamber Judgment, 25 May. Available at: https://hudoc.echr.coe.int/eng?i=001-210077 [Accessed 30 May 2025].

data from service providers also violated the Convention. This was due to its broad application beyond serious crime, the lack of prior authorisation by an independent body, and inadequate safeguards for protecting journalists' confidential sources.[258]

When multiple oversight bodies share responsibilities without clearly defined boundaries, confusion and inefficiencies often arise. This lack of clarity can lead to duplicated efforts, conflicting assessments, or, conversely, oversight gaps where nobody takes full responsibility. For example, Germany's federal intelligence services are overseen by several bodies, including the Parliamentary Oversight Panel (PKGr), the G10 Commission, the Federal Commissioner for Data Protection and Freedom of Information (BfDI), and the Independent Oversight Council. While each has a distinct mandate, their responsibilities can overlap. The G10 Commission specifically evaluates surveillance measures that may infringe on the confidentiality of telecommunications protected under Article 10 of the Basic Law. The BfDI, on the other hand, oversees data protection and reviews activities that may affect the right to informational self-determination. However, tensions sometimes arise between the BfDI and the G10 Commission due to overlapping areas, especially when a single surveillance activity affects both rights. Only the G10 Commission can assess infringements under Article 10, limiting the BfDI's authority to independently examine related data collections. This division of competence often requires complex coordination between the two oversight bodies.[259]

2.3.3.3. Transparency and data sharing between the agencies

Thirdly, the extent to which executive oversight bodies report publicly or to other branches of government varies widely across jurisdictions. For example, in Canada, the National Security and Intelligence Review Agency (NSIRA) is an independent and external review body that reviews and investigates all Government of Canada national security and intelligence activities to ensure that they are lawful, reasonable and necessary. NSIRA also investigates public complaints regarding key national security agencies and activities. NSIRA is mandated to prepare a public annual report to the Prime Minister containing summaries of its reviews, including findings and recommendations, completed during the previous calendar year, enhancing transparency.[260] However, these reports often contain redactions

258 Global Freedom of Expression, 2021. *Big Brother Watch v. United Kingdom*. Available at: https://globalfreedomofexpression.columbia.edu/cases/big-brother-watch-v-united-kingdom/ [Accessed 30 May 2025].

259 Federal Commissioner for Data Protection and Freedom of Information (BfDI) (n.d.) *Oversight landscape: Federal intelligence services*. Available at: https://www.bfdi.bund.de/EN/Fachthemen/Inhalte/Nachrichtendienste/Kontrollandschaft-Nachrichtendienste-des-Bundes.html [Accessed 30 May 2025].

260 National Security and Intelligence Review Agency *Conducting Reviews*. Available at: https://nsira-ossnr.gc.ca/en/reviews/conducting-reviews/#:~:text=Each%20year%2C%20NSIRA%20is%20mandated,during%20the%20previous%20calendar%20year [Accessed 30 May 2025].

due to national security concerns, which limits public understanding.[261] This reflects a challenge. Transparency must be weighed carefully against the imperative to protect sensitive information. This includes safeguarding human sources, past and ongoing operations, agency personnel, and international intelligence cooperation, particularly with foreign partners. Over-disclosure could jeopardise operational security and international trust. Unlike the U.S. Department of Defense, which tends to share defence and security information more openly, Canada is often more cautious, with a noted tendency to overclassify materials, even when similar content has been widely reported by foreign media.[262] The executive will need to understand the level of international cooperation of the services to carry out effective oversight. This is because a percentage of intelligence and analysis will come from overseas partners who may be working on a different political agenda than the executive. In France, during the parliamentary debates in 2015 over the new intelligence law in France, several civil society organizations raised significant concerns about potential transparency issues in intelligence oversight. One of the most pressing criticisms came from the National Oversight Commission for Intelligence-Gathering Techniques (CNCTR), which highlighted a substantial oversight gap regarding the sharing of data between French intelligence services and foreign agencies. The issue was particularly critical due to the increasing data exchanges between the Direction Générale de la Sécurité Extérieure (DGSE) and the National Security Agency (NSA), a collaboration that was formalized through the SPINS agreements signed in late 2015 between France and the US. These agreements resulted in a substantial increase in intelligence data flows, which was not subject to oversight by the CNCTR. This was because the 2015 law explicitly prohibited the CNCTR from overseeing such international intelligence-sharing arrangements. This was especially true of those involving networks of intelligence professionals, who operate with significant autonomy and are largely insulated from external scrutiny. In its 2019 annual report, the CNCTR warned that this gap in oversight created a ‘black hole’ in the intelligence oversight framework. The Commission expressed concern that this gap could allow French intelligence services to receive data from foreign counterparts, such as the NSA, that they would otherwise be unable to legally acquire through domestic procedures established by French law.[263]

261 National Security and Intelligence Review Agency, 2021. *NSIRA Annual Report 2021*. Available at: https://nsira-ossnr.gc.ca/en/annual-reports/nsira-annual-report-2021/ [Accessed 4 November 2025].

262 House of Commons Canada, 2023. *Report of the Standing Committee on National Defence: Threat Analysis Affecting Canada and the Canadian Armed Forces Operational Readiness*, p. 57. Available at: https://www.ourcommons.ca/documentviewer/en/44-1/NDDN/report-15/page-57 [Accessed 30 May 2025].

263 AboutIntel, ‘Major Oversight Gaps in the French Intelligence Legal Framework’, *AboutIntel.eu*, 2019, https://aboutintel.eu/major-oversight-gaps-in-the-french-intelligence-legal-framework/ [Accessed 30 May 2025].

2.3.3.4. Highly sensitive decisions

Highly sensitive executive decisions such as covert operations, targeted killings, or cyber operations are typically overseen through tightly controlled internal mechanisms within the executive branch. However, these oversight processes vary significantly between countries and are often limited in scope due to the classified nature of the activities. For example, in the US, the President may authorize the conduct of a covert action only if he or she determines such an action is 'necessary to support identifiable foreign policy objectives of the United States and is important to the national security of the United States.' The President must notify Congress of all covert actions and significant clandestine activities (when activity itself, as well as U.S. sponsorship, is secret) of the Intelligence Community (IC). If the President determines that it is 'essential' to limit access to a covert action finding in order to 'meet extraordinary circumstances affecting vital interests of the United States,' he may limit the notification of such a presidential finding to the chairs and ranking Members of the House and Senate intelligence committees, the Speaker and Minority Leader of the House of Representatives, and the majority and minority leaders of the Senate.[264] The recent scandal involving members of the Trump administration using encrypted messaging apps with disappearing messages, such as Signal, to coordinate military strikes in Yemen, demonstrated the challenges of the oversight of highly sensitive decisions.[265] When records of key national security decisions are deleted or never documented, it becomes nearly impossible to assess the legality, proportionality, or authorization of those actions, effectively eroding democratic oversight and enabling executive actors to operate in secrecy with little to no accountability.

2.3.4. Conclusion

There are several compelling reasons to take executive oversight seriously. It enables more targeted and informed supervision, particularly over sensitive domains such as covert operations and targeted killings. In crisis contexts, such as counterterrorism or wartime situations, executive oversight may be the most immediate and decisive form of oversight. Moreover, in countries where parliamentary or judicial oversight is weak or underdeveloped, executive supervision often represents the only viable means of ensuring a degree of intelligence accountability. In NATO countries and beyond, these structures play a crucial role in bridging operational demands with democratic governance.

264 Congressional Research Service, 2019. *Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions in Brief*. Available at: https://www.congress.gov/crs-product/R45191 [Accessed 30 May 2025].

265 Zengler, T., 2021. 'Here's what happened to those SignalGate messages', *Wired*. Available at: https://www.wired.com/story/heres-what-happened-to-those-signalgate-messages/ [Accessed 30 May 2025].

The analysis has shown that ministries, the national security advisor and presidential/prime ministerial offices play an important role. While the specific powers and roles of executive institutions differ across political systems, their involvement in areas such as budget control, leadership appointments, and operational authorization is essential for maintaining oversight integrity. Ultimately, a well-structured executive framework not only enhances the performance of intelligence services but also helps safeguard against misuse and reinforces public trust in national security governance.

The executive oversight of intelligence services faces complex and persistent challenges, particularly regarding politicisation, coordination, transparency, and the control of highly sensitive operations. These challenges highlight the tension between maintaining operational secrecy and ensuring democratic accountability. It is especially visible when executive influence risks undermining institutional independence or legal safeguards.

Executive oversight is indispensable. However, it should not be dominant. Instead, it must function in a complementary role, reinforcing, rather than replacing, parliamentary, judicial, and civic forms of intelligence accountability.

2.4. Oversight and dialogue between intelligence services and civil society[266]

Grazvydas Jasutis, Rebecca Mikova and Kristina Vezon

2.4.1. Introduction

In recent years, understandings of democratic oversight have evolved to recognize the important role that civil society plays in monitoring the security sector. Nevertheless, national security and particularly the intelligence community is still largely considered the exclusive responsibility of the executive branch. Where civil society is involved in overseeing intelligence activities, its engagement typically takes the form of conventional public accountability procedures. It generally does so through traditional means of public oversight, such as filing lawsuits in national or international courts; drafting recommendations and engaging lawmakers; raising awareness and mobilizing public opinion; and publishing investigative reports or legal analyses. These activities are essential in promoting transparency, accountability, and respect for human rights within intelligence operations.

Often, civic oversight is only briefly referred to in the larger context of oversight debates.[267] While there are some studies that focus specifically on the role of civil society organizations (CSOs) in overseeing the intelligence sector, they are often limited in scope and tend to concentrate on particular aspects rather than offering a comprehensive analysis. A recent study based on a survey of journalists and civil society actors involved in scrutinizing intelligence surveillance in Germany, France, and the United Kingdom underscores the growing relevance of civic intelligence oversight in democratic societies. The findings reveal that civic oversight, once a marginal practice, is increasingly recognized as a vital component in responding to and shaping the governance of digital surveillance.[268] In *Civil Society's Roles in Security Sector Governance and Reform*, edited by Albrecht Schnabel and Hans-Georg Ehrhart, a collection of case studies illustrates how civil society actors function as vital agents of civilian oversight. The volume highlights their

266 This article draws on key insights from DCAF's thematic brief *Rethinking Engagement Between Intelligence Services and Civil Society*. While the authors contributed to the development of the brief, additional input was provided by the following experts: Pierre Chambart, Dragan Lozancic, and David Watson.

267 Roller, S.N., Wetzling, T., Kniep, R., and Richter, F., 2023. Civic Intelligence Oversight: Practitioners'. Perspectives in France, Germany, and the UK. *Surveillance & Society*, 21/2, 189–204. Available at: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/15217 [Accessed: 5 April 2025].

268 Roller, 2023. Civic Intelligence Oversight.

contribution to promoting transparency, accountability, and inclusive governance in security sector reform processes.[269] Complementing this perspective, *Overseeing Intelligence Services: A Toolkit* by Hans Born and Aidan Wills offers practical guidance for institutional oversight bodies, while also underscoring the critical role played by civil society organizations and the media in holding intelligence agencies to account.[270] This emphasis on non-state actors is further reinforced in *Legal Standards and Best Practice for Oversight of Intelligence Agencies* by Hans Born and Ian Leigh, which outlines the responsibilities of the executive, legislative, and judicial branches in intelligence oversight. The authors argue that effective democratic control cannot be achieved without active engagement from civil society.[271] Loch K. Johnson underscores the important contribution of civil society actors, such as the media and non-governmental organizations in uncovering misconduct within intelligence agencies. Operating as external watchdogs, these actors help expose actions that might otherwise remain hidden due to the inherently secretive nature of intelligence work[272]. In the 2014 article 'From Oversight to Undersight: The Internationalization of Intelligence,' Jelle van Buuren explored the growing influence of CSOs in driving significant legislative change. Through public advocacy, independent inquiries, and critical engagement with legal frameworks, CSOs have played a key role in pushing for reforms that strengthen democratic oversight and accountability within the intelligence sector.[273]

While underscoring the importance of such traditional oversight forms, this chapter suggests that they may be complemented by other approaches which could support intelligence services wishing to enhance dialogue with civil society. It assesses the modalities of engagement between intelligence services and civil society through establishing dialogue and channel of communication, largely referring to the *modus operandi* of intelligence services. Such dialogue can have many benefits: from improving the quality of intelligence work through identifying ways to enhance the oversight and management of intelligence activity, to increasing the legitimacy of intelligence services.

269 Schnabel, A. and Ehrhart, H-G. (eds.), 2006. *Security Sector Governance and Reform: Civil Society's Role*. Geneva: Geneva Centre for the Democratic Control of Armed Forces (DCAF).

270 Born, H. and Wills, A., 2012. *Overseeing Intelligence Services: A Toolkit*. Geneva: Geneva Centre for the Democratic Control of Armed Forces (DCAF).

271 Born, H. and Leigh, I., 2005. *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*. Oslo: Publishing House of the Parliament of Norway.

272 Johnson, L. K., 2007. *Spy Watching: Intelligence Accountability in the United States*. Yale University Press.

273 van Buuren, J., 2014. From Oversight to Undersight: The Internationalization of Intelligence. *Security and Human Rights*, 24/3-4, 239–252.

2.4.2. Forms and impact of traditional oversight

Traditionally, civil society has exercised oversight over the security sector, including the intelligence sector, through several methods. Mainly, these include filing lawsuits in national or international courts, drafting recommendations and engaging lawmakers, raising awareness and mobilizing public opinion, and publishing investigative reports or legal analyses. Their impact is far reaching, and it leads to amending the legislation, reinforcing oversight, the creation of oversight institutions and protecting the human rights of citizens. Their forms of oversight can be categorized. **In the first category**, CSOs usually employ lawsuits and legal instruments to challenge surveillance powers and abusive practices by intelligence and security agencies. This is done through constitutional complaints, administrative appeals, and human rights litigation both at the national and international levels. For instance, the case of the litigation against the Federal Intelligence Service (BND) in Germany has tackled two boundaries of liberal democracy: that of legitimate actors and territorial limits to the rule of law.[274] German CSO GFF (Gesellschaft für Freiheitsrechte) is a strategic litigation NGO that focuses on protecting civil liberties in the digital age. In 2016, in cooperation with other CSOs,[275] it filed a constitutional complaint against the BND, challenging its surveillance of foreign communications under the amended BND Act.[276] GFF argued that the BND's practices violated privacy rights and disproportionately affected journalists and civil society actors abroad. In a landmark 2020 ruling,[277] the German Constitutional Court held that fundamental rights in the German Basic Law also apply to foreign nationals outside Germany, finding the BND's foreign surveillance powers unconstitutional. This led to extensive legal reforms, including stricter requirements for proportionality, a new independent oversight body, and explicit protections for journalistic sources. However, subsequent reforms in the 2021 BND Act, which were meant to implement the Court's judgment, themselves faced significant criticism. In 2023, GFF filed a new constitutional complaint, arguing that the reformed law still does not sufficiently protect fundamental rights.[278] Core concerns include: the vague definitions of surveillance purposes; insufficient protections for confidential communications (especially for journalists and lawyers);

274 Kniep, R., Ewert, L., León-Reyes, B., Tréguer, F., McCluskey, E., and Aradau, C., 2024. 'Towards democratic intelligence oversight: Limits, practices, struggles.' *Review of International Studies*, 50/1, 209–229.

275 Other organizations which were part of this alliance included Amnesty International, the European Federation of Journalists, the European Centre for Press and Media Freedom, German Federation of Journalists, German Union of Journalists, Netzwerk Recherce (nr), n-ost, Weltreporter and Freelens, Journalistinnenbund; see Reporters Without Borders (RSF) (2020) 'Reporters Without Borders leads international alliance in campaign against surveillance of foreign journalists', *RSF* 2 March. Available at: https://rsf.org/en/reporters-without-borders-leads-international-alliance-campaign-against-surveillance-foreign [Accessed: 4 April 2025].

276 Gesellschaft für Freiheitsrechte (n.d.) *BND-Gesetz zur Ausland-Ausland-Überwachung*. Available at: https://freiheitsrechte.org/themen/freiheit-im-digitalen/bnd-gesetz-2 [Accessed: 3 April 2025].

277 Bundesverfassungsgericht, 2020. *Judgment of the First Senate of 19 May 2020 – 1 BvR 2835/17 – Strategic surveillance by the Federal Intelligence Service (BND) abroad*. Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/05/rs20200519_1bvr283517en.html [Accessed: 3 April 2025].

278 Gesellschaft für Freiheitsrechte (GFF), 2023. *Constitutional complaint against new BND law*. Available at: https://freiheitsrechte.org/en/themen/digitale-grundrechte/vb_bdng_2 [Accessed: 4 April 2025].

and shortcomings in the independence and effectiveness of the oversight body. GFF emphasized that the new rules could still permit broad, untargeted surveillance and lacked strong safeguards for the protection of sensitive data. The case is currently pending before the Constitutional Court and will be crucial for setting further standards on the extraterritorial application of human rights in intelligence operations. In parallel, GFF and Reporters Without Borders also filed an application before the European Court of Human Rights (ECtHR), challenging the BND's new surveillance powers under Articles 8 and 10 of the European Convention on Human Rights (ECHR).[279] The case is pending and could further shape European standards on privacy, press freedom, and state surveillance.

Another illustrative example of oversight-related activities comes from the work of La Quadrature du Net (LQDN). LQDN is a digital rights group that has played a central role in resisting the expansion of algorithmic and bulk surveillance powers in France. The group launched several legal challenges against laws allowing mass data collection and real-time algorithmic monitoring of internet traffic. This included the predictive analysis of online behaviour patterns, particularly targeting counterterrorism laws introduced after the 2015 attacks. LQDN filed complaints with France's Constitutional Council[280] and France's Council of State,[281] challenging the constitutionality and legality of mass surveillance laws, particularly provisions related to data retention and real-time algorithmic monitoring. Although these domestic challenges achieved only partial success, they helped bring greater scrutiny to intelligence practices and paved the way for a broader challenge before the ECtHR.[282] In 2022, the ECtHR ruled that certain aspects of France's bulk data collection regime were unlawful, citing inadequate safeguards and oversight mechanisms.[283] LQDN also mobilized public campaigns to raise awareness and pressure lawmakers. Their work resulted in greater judicial scrutiny of intelligence laws, intensified public and political debate over surveillance reforms, and contributed to demands for clearer limits on the use of algorithms and metadata collection.

279 Reporters Without Borders (RSF), 2023. 'RSF and GFF file complaint against Germany and its Federal Intelligence Service Act at European Court', *Reporters Without Borders*, 14 March. Available at: https://rsf.org/en/rsf-and-gff-file-complaint-against-germany-and-its-federal-intelligence-service-act-european-court [Accessed: 4 April 2025].

280 Conseil constitutionnel, 2017. 'Decision no. 2017-648 QPC of 4 August 2017', *La Quadrature du Net et al. [Administrative access in real time to connection data]*. Available at: https://www.conseil-constitutionnel.fr/en/decision/2017/2017648QPC.htm
[Accessed: 4 April 2025].

281 Conseil d'État, 2021. 'Decision no. 393099 of 21 April 2021'. Available at: https://www.legifrance.gouv.fr/ceta/id/CETATEXT000043411127 [Accessed: 4 April 2025]; Conseil d'État (2021) 'Decision no. 428028 of 30 December 2021'. Available at: https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2021-12-30/428028 [Accessed: 4 April 2025].

282 Quadrature du Net, 2022. 'Données de connexion : recours devant le Conseil constitutionnel', *La Quadrature du Net*, 15 February. Available at: https://www.laquadrature.net/2022/02/15/donnees-de-connexion-recours-devant-le-conseil-constitutionnel/ [Accessed: 4 April 2025]; La Quadrature du Net, 2021. 'Loi Renseignement 2: nos arguments au Conseil constitutionnel', *La Quadrature du Net*, 28 July. Available at: https://www.laquadrature.net/2021/07/28/loi-renseignement-2-nos-arguments-au-conseil-constitutionnel/ [Accessed: 4 April 2025].

283 European Court of Human Rights, 2022. *C.E. and Others v. France*, Application no. 29775/18, Judgment of 24 August. Available at: https://hudoc.echr.coe.int/eng?i=001-216707 [Accessed: 4 April 2025].

The Helsinki Foundation for Human Rights (HFHR) in Poland has been actively involved in advocating for intelligence oversight and ensuring that human rights are upheld in the context of national security and intelligence operations.[284] In 2017, they filed an application to the ECtHR about Polish legislation authorising a secret-surveillance regime covering both operational control and the retention of telecommunications, postal and digital communications data for possible future use by the relevant national authorities. In particular, they alleged that there was no remedy available under domestic law allowing persons who believed that they had been subjected to secret surveillance to complain about that fact and to have its lawfulness reviewed.[285] ECtHR has concluded that the operational-control regime, the retention of communications data, and the secret-surveillance regime under the Anti-Terrorism Act in Poland violate the right to privacy (article 8 of the ECHR).[286]

The second category implies that alongside their legal advocacy efforts, CSOs actively engage in public campaigns to highlight the risks of unchecked intelligence and to advocate for stronger privacy safeguards through pressure on lawmakers. This is well illustrated by the experiences of Liberty, a leading UK CSO, which has been instrumental in challenging the Investigatory Powers Act (IPA) 2016, commonly referred to as the 'Snoopers' Charter.' The IPA grants sweeping surveillance powers to UK intelligence agencies, including the bulk collection and retention of communications data. Liberty has argued that these powers violate the rights to privacy and freedom of expression, particularly due to inadequate safeguards for journalistic and legally privileged communications.[287] The legal campaign began shortly after the IPA was enacted. In April 2018, the High Court ruled that some provisions of the Act were incompatible with EU law, prompting Parliament to amend the legislation.[288] However, in June 2019, the High Court upheld the legality of the IPA's bulk surveillance powers overall, leading Liberty to pursue an appeal.[289] The case reached a critical point in June 2022, when the High Court found that the UK security services—including MI5, MI6, and GCHQ—had unlawfully accessed individuals' communications data held by telecom providers without independent prior approval, particularly in the context of

284 Helsinki Foundation for Human Rights (HFHR). (n.d.) *Who we are*. Available at: https://hfhr.pl/en/about-us/who-we-are [Accessed: 5 April 2025].

285 Helsinki Foundation for Human Rights (HFHR), 2024. *Judgment: Pietrzak and Bychawska-Siniarska and Others v. Poland – complaints about Polish legislation on secret surveillance* [Press release]. Warsaw: HFHR.

286 Helsinki Foundation for Human Rights (HFHR), 2024. *European Court of Human Rights: secret surveillance in Poland violates citizens' privacy rights*. Available at: https://hfhr.pl/en/news/european-court-of-human-rights-secret-surveillance-in-poland-violates-citizens-privacy-rights [Accessed: 5 April 2025].

287 Liberty, 2019. 'People Vs Snoopers' Charter: Liberty's landmark challenge to mass surveillance powers heard in High Court', 17 June. Available at: https://www.libertyhumanrights.org.uk/issue/people-vs-snoopers-charter-libertys-landmark-challenge-to-mass-surveillance-powers-heard-in-high-court/ [Accessed: 3 April 2025].

288 *R (Liberty) v Secretary of State for the Home Department* [2018] EWHC 975 (Admin). Available at: https://www.bailii.org/ew/cases/EWHC/2018/975.html [Accessed: 5 April 2025].

289 Home Office, 2019. 'Judgment in investigatory powers legal challenge', *Home Office in the media*, 29 July. Available at: https://homeofficemedia.blog.gov.uk/2019/07/29/judgment-in-investigatory-powers-legal-challenge/ [Accessed: 4 April 2025].

criminal investigations.[290] The Court ruled that, going forward, such access would require independent authorization, aligning intelligence agencies with the standards already imposed on the police.[291] These developments took place against the backdrop of a 2021 ECtHR judgment, which found that aspects of the UK's bulk interception regime violated the rights to privacy and freedom of expression, in a case led by a coalition of NGOs including Big Brother Watch, Open Rights Group, and English PEN.[292] These cases made a strong case for independent oversight and robust safeguards. In parallel with its legal advocacy, Liberty has maintained a strong public-facing campaign to raise awareness about the dangers of unchecked surveillance and to press lawmakers for stronger privacy protections. Its efforts have played a key role in shaping public and parliamentary debate on surveillance in the UK.

Similarly, Bits of Freedom, a leading Dutch digital rights organization, played a central role in opposing the so-called 'Dragnet' provision in the Dutch Intelligence and Security Services Act (Wiv 2017), a law that significantly expanded the surveillance powers of Dutch intelligence agencies.[293] Targeted surveillance was already within the powers of the Dutch secret services. The new law additionally allowed for untargeted surveillance, for the systematic and large-scale interception and analysis of citizens' online communications meaning that large numbers of citizens who are not suspected of any wrongdoing could be systematically monitored.[294] Bits of Freedom launched national public awareness campaigns warning citizens about the risks of mass surveillance as well as supported and helped coordinate a grassroots movement that successfully triggered a national advisory referendum where the majority voted against the law. Though the referendum was non-binding, several changes to the law were made that were in line with the demands of its opponents.[295] In 2022, Bits of Freedom's complaint against the unlawful data retention concerning millions of people by the Dutch secret services was successful, leading the oversight committee to order the deletion of the data.[296]

290 The Guardian, 2022. 'UK security services must seek approval to access telecoms data, judges rule', *The Guardian*, 24 June. Available at: https://www.theguardian.com/uk-news/2022/jun/24/uk-security-services-must-seek-approval-access-telecoms-data-judges-rule [Accessed: 4 April 2025].

291 Liberty, 2022. 'Liberty wins landmark Snoopers' Charter case', 24 June. Available at: https://www.libertyhumanrights.org.uk/issue/liberty-wins-landmark-snoopers-charter-case/ [Accessed: 3 April 2025].

292 European Court of Human Rights, 2021. *Big Brother Watch and Others v. the United Kingdom*, Applications nos. 58170/13, 62322/14 and 24960/15, Judgment of 25 May. Available at: https://hudoc.echr.coe.int/eng?i=001-210077 [Accessed: 4 April 2025].

293 'Bits of Freedom'. (n.d.) *Home*. Available at: https://www.bitsoffreedom.nl/. [Accessed 4 April 2025].

294 EDRi, 2017. Dutch Senate votes in favour of dragnet surveillance powers. Available at: https://edri.org/our-work/dutch-senate-votes-in-favour-of-dragnet-surveillance-powers/ [Accessed: 5 April 2025].

295 Krouwel, A., 2018. *The stormy Dutch referendum experience: social media, populists and post-materialists*. Available at: https://constitution-unit.com/2018/07/24/the-stormy-dutch-referendum-experience-social-media-populists-and-post-materialists/ [Accessed: 14 April 2025].

296 EDRi. (n.d.) *Victories*. Available at: https://edri.org/about-us/victories/. [Accessed 4 April 2025].

In the third category, CSOs focus their efforts on promoting institutional reforms within intelligence oversight frameworks and contributing directly to the shaping of public policy. International Civil Liberties Monitoring Group (ICLMG) is a national coalition of Canadian civil society organizations that was established in the aftermath of the rushed adoption of the Anti-terrorist Act of 2001.[297] After Maher Arar, a Canadian citizen, was wrongfully detained and tortured in Syria at the request of the US, based on false intelligence provided by Canadian officials, ICLMG played a key role in advocating for a public inquiry. This led to the establishment of a Commission of Inquiry, in 2024, to examine the actions of Canadian officials and to recommend policy changes. ICLMG actively participated as an intervener, contributing to the oversight discussions. The Commission ultimately exonerated Arar, leading to a government apology, and recommended creation of an integrated oversight and complaint mechanisms for all Canadian intelligence and security agencies, aligning with ICLMG's advocacy efforts.[298] ICLMG has long supported the creation of an overarching body to review all government activities related to national security. In 2017 the ICLMG submitted a brief on Bill C-22, suggesting the creation of a Committee of Parliamentarians on Intelligence and National Security.[299]

In the fourth category, CSOs particularly those specializing in investigative journalism play a vital role in exposing abuse, corruption, and misconduct within the security and intelligence sectors. Their reporting uncovers illicit enrichment, procurement fraud, unlawful surveillance, and other violations of democratic norms or legal standards. By bringing such practices to light, investigative journalists not only inform the public and policymakers but also catalyse institutional responses. Bihus.Info, a leading Ukrainian investigative journalism outlet, played a key role in exposing the corruption case involving Artem Shylo, a former advisor to the Presidential Office and a Security Service of Ukraine official. Their investigation revealed that Shylo had accumulated assets worth nearly $10 million, far exceeding his official income, raising serious concerns about illicit enrichment.[300] These revelations contributed to a formal investigation by NABU and SAPO, who in April 2024 detained Shylo for allegedly leading a scheme that embezzled 94.8 million UAH (around $2.4 million) from Ukrzaliznytsia through inflated transformer procurement contracts during martial law.[301] The funds were allegedly funnelled through a shell company tied to foreign entities, causing significant losses to the

297 International Civil Liberties Monitoring Group (ICLMG), 'Home'', ICLMG. Available at: https://iclmg.ca. [Accessed 4 April 2025]

298 Government of Canada, 'Commission of Inquiry Into the Actions of Canadian Officials in Relation to Maher Arar, Canada.ca. Available at: https://www.canada.ca/en/privy-council/services/commissions-inquiry/arar.html [Accessed: 23 April 2025].

299 International Civil Liberties Monitoring Group (ICLMG), *Brief on Bill C-59: The National Security Act, 2017*, ICLMG, May 2019. Available at https://iclmg.ca/wp-content/uploads/2019/05/C-59-Senate-brief-May-2019.pdf [Accessed: 14 April 2025].

300 Bihus.Info. '10 мільйонів доларів статків у держслужбі. Розслідування про Артема Шило. https://bihus.info; Bihus.Info, 2024. Колишньому СБУшнику і фігуранту розслідування Bihus.Info Артему Шилу повідомили про підозру. [online] 2 April. Available at: https://bihus.info/kolyshnomu-sbushnyku-i-figurantu-rozsliduvannya-bihus-info-artemu-shylu-povidomyly-pro-pidozru/ [Accessed: 14 April 2025].

301 National Anti-Corruption Bureau of Ukraine (NABU), 'NABU and SAPO detain ex-presidential advisor in $2.4 million embezzlement case. Available at: https://nabu.gov.ua [Accessed: 10 April 2025].

state.[302] This case illustrates the vital role of investigative journalism in exposing high-level corruption and triggering institutional accountability measures in Ukraine. The most striking example is perhaps the New York Times's article that led to the Church Committee.

Creation of the Church Committee in US[303]

In 1974 Pulitzer Prize winning journalist Seymour Hersh published a frontpage *New York Times* article. He claimed that the CIA, directly violating its charter, conducted a massive, illegal domestic intelligence operation during the Nixon Administration against the antiwar movement and other dissident groups in the United States, according to well□placed Government sources. A special CIA unit had compiled intelligence files on at least 10,000 Americans, operating under the direct authority of Richard Helms, who at the time of the surveillance served as Director of Central Intelligence and later became U.S. Ambassador to Iran. According to sources, a review of domestic files ordered by Helms's successor, James R. Schlesinger, uncovered evidence of numerous other unlawful activities carried out by the agency within the United States from the 1950s onward, including break-ins, wiretaps, and the covert interception of mail. Publication of these findings prompted Congress to establish a committee of inquiry.

On January 21, 1975, Senator John Pastore introduced a resolution to establish a select committee to investigate federal intelligence operations and determine 'the extent, if any, to which illegal, improper, or unethical activities were engaged in by any agency of the Federal Government.' The Senate approved the resolution, 82-4. Majority Leader Mike Mansfield cautioned the Senate 'against letting the affair become a 'television extravaganza.'' He and Republican leader Hugh Scott carefully selected committee members, balancing experienced lawmakers with junior members and ensuring that members represented a variety of political viewpoints. When Philip Hart declined to lead the committee for health-related reasons, Mansfield selected Democrat Frank Church of Idaho to serve as chairman. A sixteen-year member of the Committee on Foreign Relations, Church had co-chaired a special committee to critically examine the executive branch's consolidation of power in the Cold War era. Church recognized the strategic value of the nation's top intelligence agencies and was also mindful of the need for American institutions to function within the confines of U.S. constitutional law. He had aggressively lobbied to lead the investigation.

302 The Kyiv Independent. 'Former advisor to Presidential Office charged with embezzling $2.4 million', April 2024. Available at: https://kyivindependent.com [Accessed: 14 April 2025].

303 Hersh, S.M., 1974. Huge C.I.A. operation reported in U.S. against antiwar forces, other dissidents in Nixon years. *The New York Times*, 22 December. Available at: https://www.nytimes.com/1974/12/22/archives/huge-cia-operation-reported-in-u-s-against-antiwar-forces-other.html [Accessed 6 May 2025]
U.S. Senate Historical Office, A history of notable Senate investigations: the Church Committee. [pdf] Washington, D.C.: U.S. Senate. Available at: https://www.senate.gov/about/resources/pdf/church-committee-full-citations.pdf [Accessed 6 May 2025]

CSOs are, of course, engaged in many different ways. However, these activities constitute one of the most important means through which the conduct of intelligence services can be scrutinised and how an accountable and responsive intelligence service should work. The above-mentioned strategies are critical for ensuring effective public oversight of the security sector. Nevertheless, they are generally initiated by civil society, rather than intelligence services. This can act to absolve intelligence organisations of the need to establish dialogue with civil society and prevent it from drawing upon the expertise that civil society can offer. Indeed, when implemented alone, traditional forms of public oversight conducted by civil society over the intelligence sector can create an adversarial relationship between the two, thwarting mutual understanding and trust. Such approaches have merit. But they are limited in their ability to achieve direct engagement between civil society and intelligence services, and thus in fostering understanding and mutual dialogue between the two.

2.4.3. *Raison d'être* for dialogue between civil society and the intelligence community

A structured and sustained dialogue between civil society and the intelligence community can serve multiple purposes in enhancing democratic governance, transparency, and accountability in the intelligence sector:

- **Avoid politicization:** dialogue limits activities of the executive branch that may lead to the politicization of the intelligence services or misuse for its own political ends. Policymakers may neglect intelligence products that do not confirm the political masters' agenda and the engagement of CSOs can reinforce objectivity versus policy influence and persuasion.

- **Enhance awareness on the security needs of civil society:** civil society possesses technical expertise that intelligence services rarely draw upon. Specialized CSOs, often composed of former practitioners, can contribute to analysing national security threats, and can formulate proposals responding to the security needs and challenges of broader society. They can analyse legal and institutional frameworks governing the activity of intelligence services, in particular regarding information classification and oversight.

- **Increase legitimacy of and trust in intelligence services:** the establishment of platforms for mutual dialogue between civil society and the intelligence community can enhance the legitimacy and credibility of latter. CSOs can play an important role in promoting societal awareness and understanding of the role that intelligence services play in ensuring national security. In particular, specialized CSOs can contribute to the development of strategic communication policies which ensure that intelligence services effectively communicate the nature of their work to the public.

- **Facilitate professionalism and integrity of intelligence services:** CSOs dealing with ethics and security sector management can contribute their expertise to develop ethics frameworks for intelligence services, in particular codes of ethics and conduct.

- **Provide a platform to deal with historic grievances:** In many transition states, intelligence services must confront a past characterized by a confrontational relationship with society. In some cases, intelligence services stand accused of committing historic injustices, and are viewed with suspicion by civil society. Providing platforms for mutual dialogue with civil society can help overcome such historical grievances, and can facilitate communication with civil society on the nature and progress of intelligence reform processes.

2.4.4. New forms of dialogue

Several strategies exist which could be leveraged by intelligence services to enhance dialogue with civil society. The core aim of such approaches is to move civil society-intelligence sector relations beyond traditional forms of oversight, towards mutual cooperation and dialogue. In combination with traditional forms of oversight, such approaches can open intelligence services to the untapped potential of civil society; can enhance public trust, and act as a conflict prevention mechanism by providing a platform to address historic grievances and communicate intelligence reform processes. This approach attempts to deconstruct the perception of civil society and intelligence services as 'adversaries' by considering their shared goals and common purpose: ensuring the effective provision of security. The below details several strategies which could be employed, or otherwise advocated for, by intelligence services. Where applicable, case studies are also provided.

Civilian oversight councils

Some countries have considered creating Civil Oversight Bodies, composed of civil society representatives who are mandated under law to oversee intelligence services. As part of their mandate, these bodies must also establish direct channels of communication with intelligence services. Two examples of such institutions exist: the Croatian Council for Civilian Oversight of the Security and Intelligence Services; and the North Macedonian Council of Civilian Supervision. In both cases, these bodies are not fully independent, being accountable to the national parliament. If established as an independent body, such an institution would be free of political party affiliations, and thus more objective in their analysis of and interaction with intelligence services. This could potentially serve a useful means through which dialogue and mutual trust between civil society and intelligence services could be improved.

Case Study: Croatian Civilian Oversight Council

Croatian 2006 Security-Intelligence System Acts provides for three oversight bodies: a standing parliamentary oversight committee, an administrative oversight body and the Civilian Oversight Council (COC). The COC's mandate is two-fold: assure the legality of intelligence activities and the legitimate use of special powers. The COC consists of seven members chosen to serve a four-year term by the parliament after an open selection process. It is accountable to the parliament, staffed by former intelligence personnel, as well as civil society representatives, and its work is overseen by the parliament's intelligence oversight committee.

The Council played an important role in several high-profile cases of abuse of special powers. On two occasions in 2004 and 2007, separate court proceedings filed by victims of abuse acknowledged the valuable contribution of the Council in establishing the facts and the court's rulings.

The Civilian Oversight Council has since taken on a more complementary role to that of the parliament. It mainly investigates individual complaints from citizens, with high-profile cases generally addressed by the parliamentary oversight committee. The COC has the authority to review any documents and interview intelligence officials.

While the establishment of a civilian oversight council would require a legislative amendment(s), an alternative approach might involve the inclusion of civil society representatives in expert oversight bodies. Within the Euro-Atlantic sphere, such bodies are widespread.[304] But they typically include individuals with legal and judicial expertise (former judges, prosecutors, politicians, senior law-enforcement officials). Expanding this requirement to include representatives of civil society, as in the case of the Croatian Council for Civilian Oversight, would enable civil society engagement without a need for legislative amendments.

Roundtable discussions

Intelligence services may consider convening roundtable discussions with civil society organizations. While in practice this remains rare, it provides a unique opportunity to build trust between intelligence officials and civil society. It can help ensure that civil society understands the broader issues at stake and is able to consider the perspective of intelligence agencies. In Croatia, the intelligence service introduced annual round-table discussions between senior intelligence officials and CSOs. The initiative has been viewed positively by both sides, and has been said to result in greater transparency on the part of intelligence services, with an increase in the number of publicly released documents and declassified information.

304 Belgium – Standing Intelligence Agencies Review Committee, Netherlands, Norway, Portugal and, Sweden.

Alternatively, in the Unites States, the Office of Civil Liberties, Privacy and Transparency convenes discussions with civil society following disclosures of newly declassified documents by the Director of National Intelligence. This provides context to the documentation, and allows for civil society to ask related questions. In addition, such discussions provide an opportunity to address concerns related to surveillance and the use of other intrusive methods by intelligence services. It also provides civil society with an opportunity to present their perspective on the issues. A certain level of engagement can also be observed in France, with its intelligence officials present during the 'La Fabrique Défense' event, to 'inform, discuss and debate' the security issues with wider audience.

Provision of information by intelligence services

Publishing declassified annual reports on the activities of intelligence service has become a widespread practice to facilitate information sharing with civil society. For example, the Latvian Constitution Protection Bureau publishes annual reports on its activities, while Croatian agency permitted visits to their premises by students, CSOs and international delegations, such as members of parliamentary oversight committees. Annual reports are also an established practice in Czechia, France and Slovakia amongst others.

In addition to this, clear and transparent procedures for the declassification of information are important for facilitating the engagement of civil society with intelligence matters. For example, the French intelligence community has consulted several historians and journalists in managing the progressive declassification of their archive.

Expert reports and recommendations by CSOs

CSOs frequently focus on specific topics and areas of public concern such as civil liberties, privacy, or online surveillance (interception of personal communication). Their analyses, reports and recommendations can help intelligence agencies to improve their institutional functioning and operations.

Engagement of CSO experts in supporting work of intelligence services

Intelligence services can make use of the capacities of civil society by requesting their help in specific research activities in relation to national security. CSOs may possess knowledge of local developments and the factors and causes that shape them, exposing intelligence services to information that would otherwise be hard to procure.

Establishing relationships with academic communities

Another avenue for facilitating engagement between intelligence services and civil society is fostering cooperation with the academic community. Such an approach may include the provision of internships to university students. For example, the Czech Intelligence service (BIS – Bezpecnostni Informacni Sluzba) has, since 2017, offered three rounds of internship positions for university students. In 2018, the BIS has also hosted a lecture in cooperation with the Plzen law faculty on the topic of 'Legal Status and Functioning of the BIS within the Czech Security System.'

Another example includes that of the State Security Department in the Republic of Lithuania, which has initiated a joint project with Vilnius University entitled 'Intelligence officer for a Week'. Sixty students were briefed about the challenges of Lithuanian national security and the specifics of intelligence activities.

Hosting of and participation in public events

Intelligence services can increase awareness and trust by hosting events available to the public. For example, the State Security Department of the Republic of Lithuania supported the initiatives of the hundredth anniversary of the restoration of the statehood and implemented projects to increase awareness of intelligence service from a historical perspective. It initiated of and contributed to the production of the documentary '*Shadow Front*'. A public event was organized to mark the hundred-and-twenty-fifth anniversary of the pioneer of Lithuanian intelligence, Mikalojus Lipcius. The French intelligence community has a practice of receiving accredited journalists, commissions polls about its popularity and promotes its image by being closely associated with TV shows.

Establishing online platforms

One of the major obstacles to systematic engagement between civil society and intelligence services is the absence of a platform through which regular communication can be maintained. Currently, it remains common practice for CSOs to publish reports on intelligence agencies, but without any platform for these agencies to follow up on identified issues and concerns. Establishing a digital platform in which the intelligence service and CSOs could act to foster cooperation and understanding would be to society's advantage. Over time, such digital platforms might lead to the formation of a community of practice among CSO representatives on intelligence matters, with whom intelligence services could discuss related issues.

2.4.5. Conclusion

Traditional forms of oversight, such as legal advocacy, public campaigning, strategic litigation, and critical reporting have played a vital role in strengthening the democratic accountability of intelligence services. As demonstrated through numerous impactful cases given above, CSOs have successfully challenged unlawful surveillance practices, prompted legal reforms, and raised public awareness about the implications of intelligence activities for privacy and human rights.

However, relying solely on these conventional mechanisms can foster an adversarial dynamic between civil society and the intelligence community. It may hinder trust-building, mutual understanding, and constructive collaboration. Intelligence agencies have historically remained isolated from civil society, missing valuable opportunities to benefit from its technical expertise, social insights, and legitimacy enhancing functions.

The authors here have suggested a complementary approach. The development of structured, transparent, and inclusive forms of dialogue between intelligence services and civil society. Through mechanisms such as civilian oversight councils, roundtable discussions, collaborative academic programs, expert consultations, and online engagement platforms, intelligence agencies can move toward a more open posture that supports trust, professionalism, and responsiveness to societal concerns. Such engagement should not replace independent oversight, rather they should enrich it. Intelligence operations are increasingly complex and transnational, and societal trust in institutions is often fragile. In this context the development of a meaningful dialogue between civil society and the intelligence services is not only beneficial but it is essential for the future of democratic security governance.

Photo by Gorodenkoff, stock.adobe.com

Part III: Case studies from the Euro-Atlantic region

The Euro-Atlantic region includes a diverse range of intelligence and security governance models, each shaped by unique historical experiences, political traditions, and security challenges. This section presents a set of case studies that illustrate how different states organise, mandate, and oversee their intelligence services, including those with law enforcement functions. While the specific institutional frameworks vary widely from parliamentary committees with broad investigative powers to specialised ombudspersons and multi-layered oversight architectures, common democratic principles underpin these systems: legality, accountability, proportionality, and respect for fundamental rights.

The case studies demonstrate that effective oversight must be context-sensitive, reflecting each nation's constitutional framework, political culture, and threat environment. By examining these national experiences, this section highlights both best practices and ongoing challenges. The diversity of approaches underscores the necessity of tailoring oversight systems to local realities, while reaffirming the central role of transparency, checks and balances, and multi-actor engagement including parliaments, judiciaries, executives, civil society, and the media. It is these taken together that allow intelligence services to operate within democratic boundaries effectively while safeguarding national security.

3.1. Polish case study: Intelligence and law enforcement mandate

Grzegorz Malecki

3.1.1. Material scope: 'Special Services'

Polish legislation uses the term 'special services', as a collective term for the five civil and military foreign intelligence and security and counterintelligence services, as well as (since 2006) the national anti-corruption service. This concept occurs in the so-called 'competence laws' concerning these five services. None of the acts gives a definition, limiting themselves to granting a specific status of 'special service'.

Currently (after the reorganizations in 2002 and 2006), the following agencies enjoy the status of special services in Poland: the Internal Security Agency (*Agencja Bezpieczeństwa Wewnętrznego*, or ABW), the Foreign Intelligence Agency (*Agencja Wywiadu*, or AW), the Central Anti-Corruption Bureau (*Centralne Biuro Antykorupcyjne*, or CBA), the Military Counterintelligence Service (*Służba Kontrwywiadu Wojskowego*, or SKW), and the Military Intelligence Service (*Służba Wywiadu Wojskowego*, or SWW). The only common feature of these special services is their democratic oversight, which is specifically built around two supervisory bodies: SKSS and the government KSS.

There are no specific tasks or powers that would define the ABW, AW, CBA, SKW, and SWW as a uniform group of services. There are, in this category, typical intelligence services (the AW, SKW, and SWW), an intelligence and police service (the ABW), and a police service (the CBA). The ABW and CBA have law enforcement powers. Thus, in the current legal framework, special services are those that require special oversight and control.

The activities of individual services, their tasks, functions, powers and principles of service are regulated by the following competence laws:

- Act on the Internal Security Agency and the Foreign Intelligence Agency of 24 July 2002.
- Act on the Military Counterintelligence Service and the Military Intelligence Service of 9 June 2006.
- Act on the Central Anti-Corruption Bureau of 9 June 2006.

There are provisions specifying the mode, principles and scope of oversight and the control of certain aspects of their activities by external authorities. Of special importance are their use of so-called operational control measures, that is offensive surveillance techniques (see further below).

In addition, the Act on ABW and AW contains provisions around the activities of the KSS, including its tasks, composition, powers and scope and method of operation.

3.1.2. The oversight and control apparatus of the state over special services: General outline

The range of bodies with oversight and control powers over special services is extensive and includes entities such as: the Prime Minister who exercises direct general administrative control; some ministers;[305] the public prosecutor's office; the courts (Constitutional Tribunal, administrative and common courts); competent parliamentary committees; and bodies appointed on the basis of the Constitution by the Sejm, that is, the Supreme Audit Office and the Ombudsperson.

A characteristic feature of the institutional model developed after 1990 in Poland is the lack of a comprehensive, framework law on the system of oversight and control of the special services. The mandate, tasks and powers of the various oversight and control bodies do not form a comprehensive and coherent structure that can be called a system. Their tasks and control functions towards special services are in most cases not the main objective of their activities (except for SKSS and KSS).

The common, constitutive competence of all special services, serving the implementation of their essential statutory tasks is the power to conduct so-called 'operational-reconnaissance activities' (hereinafter operational activities). The attention and activity of the oversight and control authorities is varied. However, oversight is very unevenly distributed among the different bodies in terms of tools, mode, scope of control activities, and instruments of impact on individual services.

3.1.3. Operational-reconnaissance activities

An explanation of the concept of 'operational activities,' as shaped by both legislation and practice in Poland's special services, is crucial for grasping the mechanisms and principles of their oversight and control. These activities are treated as the fundamental activity of the special services, despite the fact that it is also an essential tool for the operation of six other police services.

305 The Minister Coordinator for Special Services, the Minister of National Defense, Finance, Internal affairs and Foreign Affairs, as members of the opinion-giving and advisory body KSS.

In these circumstances, it is significant that Poland's legislation is silent on the definition of operational-reconnaissance activities, and therefore the scope of meaning has been shaped by the literature and practice. It is assumed that these are 'activities whose main purpose is to prevent, identify and detect the perpetrators of crimes', which are extra-judicial, technical-tactical activities and practices of authorized services aimed at preventing and combating crime. A characteristic feature of this approach is the perception of the activities of special services in relation to the process (trial) function.

Therefore, operational activities can be defined as a catalogue of the powers of designated services to take action. This includes activities aimed at the secret acquisition, collection, processing and the verification of information relevant to, in broad terms, state (national) security.

In practice, the following catalogue of activities introduced in the laws is referred to as operational-reconnaissance activities:

- **Taking advantage of the (usually secret) assistance of persons who are not officers, soldiers or employees of special services, in other words informants or agents** (human sources of information). This secret cooperation and the persons involved are subject to specific strict legal protection measures. The application of this method is to be vested in all special services.

  In this context, an important element of Poland's model is the statutory ban on cooperation between certain categories of public officials and the intelligence services. This includes parliamentarians, people holding managerial positions in the state, judges and prosecutors or journalists. An exemption from this prohibition may be granted in situations justified by national security, provided the Head of the service obtains the prior consent of the Prime Minister.

- **Operational control** is another key term without a statutory definition. It covers a wide range of offensive surveillance activities and techniques used by special services and law enforcement services. It is conducted in secret and consists of: the obtaining and recording of conversations conducted *via* technical means, including telecommunications networks; the obtaining and preservation of images and sounds of persons from premises, means of transport and other non-public places; the obtaining and preservation of the content of correspondence, including correspondence via electronic means of communication; the obtaining and preservation of data included in IT data carriers, telecommunications terminal equipment, IT and telecommunications systems; and obtaining access to and control of the content of parcels.

  An important aspect of the application of operational control by special services is the unspecified (relatively open) catalogue of crimes against which operational control is applied and the *unambiguous dependence of the purpose on obtaining evidence of crimes*. This approach clearly distinguishes the Polish model from

most Euro-Atlantic countries. Elsewhere, the surveillance activities of intelligence services are to obtain information for state security, without connection with criminal prosecution of perpetrators of crimes. Another important, specific aspect of the model is the open catalogue of technical measures used in operational control, which is a field for freedom of interpretation and abuses, and a serious challenge for oversight and control authorities.

The application of operational control within the definition given above is a competence of ABW, SKW and CBA. AW and SWW have, instead, a mandate to carry out tasks outside the country. But they may, in certain cases, carry out some operational control activities in the country *via* (respectively) ABW and SKW.

- **Acquisition and processing of personal data** without the knowledge of the data subjects. All special services have the competence to use personal data, and the remaining six are also authorized to conduct operational and reconnaissance activities. This power includes the maintenance and uses of databases, as well as collections maintained by other entities.

- **Obtaining telecommunication data.** There are two categories of data and special services are given access to each of them on different terms. The first category is *the content of conversations or messages exchanged by users of telecommunications networks*. Access to them is possible as part of ongoing criminal proceedings on the decision of the public prosecutor or court conducting them. Alternatively, access is given in the course of operational-reconnaissance activities as part of pre-trial proceedings conducted by a service (no criminal proceedings are pending), with the consent of the court.

  The second category of telecommunications data is metadata, that is, data related to transfers and network users, which are generated in the telecommunications network. Obtaining access to this type of data does not require the authorization of any external entity (details will be discussed below).

  Access to telecommunications data can be obtained by domestic special services, namely ABW, SKW and CBA.

- **Controlled purchase ('sting operation').** A proposal is made to a suspect to purchase or sell items derived from a crime or prohibited by law: this would include allowing a suspect to give or accept a bribe. ABW, SKW and CBA are authorised to use it. The prosecutor is involved in the authorisation process of this measure.

- **Controlled delivery** consists in the secret monitoring (surveillance) of the manufacture, movement, storage and marketing of objects of crime. The aim is to document criminal activity or to determine the identity of persons participating, as well as the acquisition of objects of crime. In authorizing the

use of this tool, the prosecutor takes part. Services authorised to use controlled delivery are ABW, SKW and CBA.

- **Use documents, which preclude the identity** of officers and soldiers and persons cooperating with the services. All special services have the power to do this.

- **Obtaining financial data.** Financial data could be bank secrecy; data processed by banks; information concerning agreements on securities accounts; agreements on money accounts; insurance agreements or other agreements concerning trading in financial instruments. It also includes the personal data of persons who concluded such contracts, processed by the authorised entities. ABW and CBA have this power.

  The provisions of the competence laws and the Act on the Protection of Classified Information place particular emphasis on the protection of forms and methods of operational activities. This includes data identifying officers and soldiers of these services and their informants. Access to them is generally prohibited to any external bodies, save in exceptional circumstances described in laws. In these cases, access can be obtained by a court or public prosecutor or (with much more difficulty) the Prime Minister or the Minister Coordinator for Special Services (hereinafter the Minister Coordinator).

3.1.4. Special services performing law enforcement functions

Of the five special services, ABW and CBA have law enforcement powers. For this reason, the dominant function, determining their profile and paradigm of activity is specific to law enforcement services.

Description of tasks and powers of ABW. The statutory competence of the ABW is, in the most general sense, the protection of the internal security of the state and its constitutional order. The list of tasks and powers of the ABW, including a general catalogue of crimes whose criminal prosecution is within its competence, is primarily specified in the Act on the ABW and AW.

Description of the tasks and powers of the CBA. The statutory competence of the CBA is to combat corruption in public and economic life, in particular in state and local government institutions. Its purpose is also to combat activities that undermine the economic interests of the state. The list of tasks and powers can be found in the CBA Act.

3.1.5. Control by executive bodies

Poland is one of the few EU and NATO member states without a permanent, integrated, and unified system for the management of the intelligence services, as they are defined and understood by the Euro-Atlantic community. The current organizational set-up was created in 1997 and has continued to operate without much change since.

The organizational and functional set-up is created by regulations scattered across a number of laws defining the powers in the sphere of oversight and control over the services of various state authorities.

The powers of the President of the Republic in the scope of oversight and control of special services are small. They boil down to the exercise of opinion-giving functions in the few procedures related to the programming of the activities of services and their personnel policy.

The President of the Council of Ministers (Prime Minister) has the broadest powers over special services, being their main disposer and the head of the entire government administration, to which they also belong. ABW, AW and CBA are directly subordinated to the Prime Minister. The direct superior of the military services, meanwhile, SKW and SWW, is the Minister of National Defence. Nevertheless, the Head of each of the special services is appointed and dismissed by the decision of the Prime Minister (in the case of SKW and SWW after having consulted the Ministry of National Defence).

The scope of the Prime Minister's powers is extensive and covers the main areas of activity of special services, in particular: the programming of their activities; the coordination of cooperation between special services and their cooperation with other bodies; organizational matters (approving the statutes of ABW, AW, and CBA, and consenting to the statutes of SWW and SKW prepared by the Ministry of Finance); and certain personnel matters. The specific powers of the Prime Minister related to the implementation of the operational-reconnaissance activities of intelligence services (without CBA) include the right to express consent:

- to the recruitment of persons otherwise subject to a statutory prohibition on cooperation, including journalists, as secret informants.
- for officers of these services to perform functions related to being members of management and control bodies of commercial law companies and cooperatives.

The powers of the Prime Minister presented above are not complete, but they include points referred to in the dispersed regulations of some acts (mainly competence laws). A number of other competences are in the legislation and practice concerning the operation of the government administration, whose superior is the Prime Minister.

Both the Prime Minister and the Minister Coordinator (if appointed) acting on his/her behalf share their control powers with the Minister of National Defence, who is the direct supervisor of Heads of military services (SKW and SWW). Therefore, the control status of the Ministry of National Defence should be considered limited, and its scope covers primarily programming, organizational and certain personnel issues.

The Minister Coordinator plays a key role in the executive control system towards special services. Since 1997, there has been a (quite inconsistent) practice of appointing the so-called 'task minister', responsible for the control and coordination of special services. However, this minister is not a permanent feature of the Polish government structure. In fact, the Minister Coordinator for Special Services is appointed on a case-by-case basis on the strength of a competence decree by the President of the Council of Ministers. This body does not constitute a permanent institutional body, constituted under a legal act of statutory rank. It means an ephemeral and unstable solution.

The current scope of powers, formed in the decree of November 2015 and reproduced in subsequent regulations, including the current ones (from 2023) determines the status of the Minister Coordinator. It also determines the scope of his tasks, covering three separately systematized main areas of competence: control, auditing, and coordination of activities of special services, as well as assisting the Council of Ministers in shaping the main directions of government policy regarding the activities of special services.

Powers are related primarily to the programming of the work of the special services, for example: setting strategic directions for the development and operation of special services; elaboration of special services activity programs in the field of state security; approval of annual work plans prepared by the heads of the different special services; or setting goals and directions for the development of international cooperation of special services and assessing the effects of this cooperation.

The Minister Coordinator is also responsible for monitoring the system of protecting classified information, a system primarily managed by the special services. Within this system, ABW and SKW act as the key state security services, serving as the authorities that issue security clearances to citizens seeking access to state secrets. The Minister Coordinator was also appointed to perform the task of the body dealing with complaints against the activities of special services, addressed to the Prime Minister. It should be noted that the procedure for dealing with these complaints results from the general provisions contained in the Code of Administrative Procedure, relating to the rules for submitting and handling complaints against administrative action

The scope of the audit tasks of the Minister Coordinator is based on the applicable auditing regulations in the government administration, in relation to central government administrative bodies and the Act on the protection of classified

information. The Minister performs audit proceedings in special services on the terms and in the manner specified in the Act on auditing government administration.

The competence decree of the Minister Coordinator also provides for extensive coordination tasks. This is particularly for taking measures to ensure: the cooperation of special services within the scope of their competences and tasks; organizing and ensuring the cooperation of special services with other services and institutions performing tasks in the field of state security; ensuring optimal conditions for the cooperation of special services with special services of other countries and international organizations; and drafting and preparing legislation on special services or resolving disputes concerning powers between special services.

The above catalogue of control, auditing and coordination tasks is supplemented by a short catalogue of additional tasks. These include, in particular, the need to conduct international cooperation with authorities of other countries and international institutions dealing with coordination, oversight and control of special services.

In order to carry out these precisely defined tasks, the Minister Coordinator was granted an extensive catalogue of executive powers related to obtaining information from special services and issuing decisions on specific matters. Special services are obliged to provide, at the request of the Minister, all information, documents, analyses and periodic reports either on a particular case or a type of case. They must also give information on budget planning and its implementation and personnel policy as it is conducted in individual special services. The Minister is also entitled to apply to members of the Cabinet and government administrative bodies to provide information necessary for the control, auditing and coordination of the activities of the special services. The scope of powers in the field of obtaining information is complemented by a competence to familiarize with information that may be important for the security and international position of the Republic of Poland, collected by ABW, AW and SKW and SWW, as well as information containing the results of CBA analyses within the scope of its competences.

The Minister Coordinator was also authorized by virtue of the competence decree to issue decisions on behalf of the Prime Minister terminating appeal proceedings regarding personnel security clearance and industrial security certificate. All this was conducted on the basis of the Act on the Protection of Classified Information.

The most firmly established and enduring element of executive oversight is the Board for Special Services (KSS). It is ‘an opinion-giving and advisory body of the Council of Ministers in matters of programming, control and coordinating the activities of special services’ created in 1997. The current status, scope and principles of operation of the KSS are regulated by chapter 2 of the Act of the ABW and AW. It is the only body in the current apparatus of oversight and control over special services, formed on the basis of the Act.

The Board consists of: President of the Council of Ministers, as chairman and the Secretary of the Board (appointed by the Prime Minister). There are then five permanent members: the Minister of the Interior; the Minister of Foreign Affairs; the Minister of National Defence; the Minister of Finance; and the Presidential Head of the National Security Bureau. There is also the Minister Coordinator, if appointed. The meetings of the Board are also attended by the heads of the special services and the Chairman of the Sejm Special Services Committee (SKSS). The President of the Republic of Poland may delegate his/her representative to participate in the meetings of the Board. However, this delegate would be in an observer role and, unlike the heads of services and the chairman of the SKSS, this delegate would have no right to vote within the committee.

The Board: formulates assessments or expresses opinions on personnel policy issues (appointment and dismissal of the heads of special services); deals with the programming and accounting (reports) of their activities; looks at legislation on special services, coordination of services activities; as well as activities in connection with the Police, the Border Guard, the Marshal Guard, the Military Police, the State Protection Service, the National Revenue Administration, financial information authorities and the reconnaissance services of the Armed Forces of the Republic of Poland. The Board organizes, too, the exchange of information relevant to security and the international position of the Republic of Poland between government administration bodies and the protection of classified information.

The structured scope of the competences of the Minister Coordinator, performing the tasks entrusted by the Prime Minister, create a coherent and transparent system. These cover key aspects of the services' operation, which can be the foundation for an efficient executive apparatus under the Prime Minister's control. The main problem, however, is the lack of its statutory legitimacy, including independent control powers (not ceded by the Prime Minister). Above all, there is the lack of an executive auxiliary body subordinate to the Minister Coordinator through which it will carry out the tasks and competences entrusted to him or her. The administrative service of the Minister Coordinator and the Board for Special Services is provided by the Chancellery of the Prime Minister, within its own budget and personnel resources. In practice, this means that the Minister Coordinator and the Secretary of the Board have a common auxiliary apparatus. It is organized in the form of the National Security Department. Its staff consists of civil servants in the Chancellery and officers delegated from individual services. This limited staff, about 30 persons, can only carry out a small percentage of the extremely wide range of tasks indicated in the competence decree of the Minister Coordinator.

3.1.6. Public prosecutor's office and control functions

An important element in the control of the executive over the special services is the public prosecutor's office. It performs control functions as an instrument of executive power, which results from its location inside the government apparatus. Formally, the Head of the prosecutor's office is the Attorney General or the Public Prosecutor General. He is also the Minister of Justice, but the work of the public prosecutor's office is headed by the National Public Prosecutor, who is the First Deputy Public Prosecutor General. His or her competence, according to present regulations, is to perform all control functions of the public prosecutor's office towards the special services.

The public prosecutor's control tends to involve the most intrusive methods of operational-reconnaissance activities of the special services. These include: operational control; controlled purchases and controlled deliveries; obtaining telecommunications data relevant to criminal proceedings; and obtaining secret data, processed by banks and financial institutions.

In the case of operational control, the participation of the National Public Prosecutor consists in participating in the authorization of a given activity by the court. This includes consenting to requests submitted by the head of the service, agreeing to orders in urgent cases, authorising extensions, and participating in court hearings. The Prosecutor also receives certain categories of materials along with information about their destruction. He/she shall also keep a register of provisions, written consents, orders and requests for operational control.

In the authorization procedure a controlled purchase and a secretly controlled delivery, the role of the National Public Prosecutor consists in consenting to the order of the service head and receiving materials obtained in its course.

With regard to telecommunications data, the National Public Prosecutor receives from the service head the data that are relevant for criminal proceedings and decides on the scope and manner of their further use.

The role of the National Public Prosecutor in obtaining access to information from banking and financial institutions consists in agreeing to the request of a service head to postpone the obligation to inform persons who are affected by the data collected to further operational-reconnaissance activities.

An obvious element of the public prosecutor's control is indirect and comes out of the Prosecutor's role in some criminal trials. This occurs when a case is initiated based on findings by the special services, or when the services carry out investigative activities during the preparatory proceedings under the prosecutor's supervision. In such situations, the prosecutor is formally the authority responsible for the proceedings, even if the services conduct much of the work in practice.

3.1.7. Parliamentary oversight

According to the legislation, which must be congruent with the Constitution, the activities of the Council of Ministers and its members and the government administration are subject to the Sejm, the lower house of Parliament. The control function of the Sejm is carried out in two ways. Firstly, indirectly, the Sejm shapes the entire oversight and control system in the state, including the appointment of two constitutional bodies exercising control, namely the President of Supreme Audit Office (NIK) and the Ombudsman (RPO).

Above of all, however, the control function is exercised in direct terms. This means the performance of oversight activities by the Sejm and its committees and MPs. A Parliamentary Committee for Special Services (SKSS) is responsible for oversight of the activities of the special services and the government in the area of their control.

The legal basis of the SKSS is in the standing orders of the Sejm, so there is no statutory authorization. Indeed, its mandate is relatively weak and the committee generally unstable. Its tasks, composition and principles of operation are subject to fairly easy and frequent changes, conditioned by the current political design in the Sejm and the political interest of the parliamentary majority at any given time.

Although appointed on the basis of the Standing Orders of the Sejm, this committee has a special character, different from other Sejm committees. Unlike most of them, some of its competences are anchored in laws, for example, the opinion-giving powers in the procedure of appointing and dismissing the heads of ABW, AW, SKW and SWW and their deputies are specified in the competence laws concerning these services.

In formal terms, the committee is one of the permanent bodies of the Sejm; it is internal and auxiliary in nature. In reality, it is granted far-reaching independence, and its role is to represent the Sejm. It often stands in for the Sejm instead of assisting it. Unlike other parliamentary committees, the Sejm does not have the power to change or correct the position of the Parliamentary Committee for Special Services. The independence of the Committee can be seen in its statutory anchorage, the secrecy of its meetings, and its specific powers and duties (which it exercises in an independent manner). For example, the resolutions it adopts when presenting opinions on prospective heads of special services and their deputies are conclusive and incontrovertible. The Sejm does not have the power to amend or repeal them; nor is it in a position to pass a resolution supplanting the opinion expressed by the Committee. The standing orders of the Sejm stipulate that the sittings of the Parliamentary Committee for Special Services may only be attended by members. This is not the case with other committees.

In the case of SKSS, there is also a specific obligation for members of the committee to have personnel security clearance for top-secret information, issued by ABW after conducting the vetting procedure. MPs only have access to information marked 'secret' under the Act, by passing the vetting procedure.

The current standing orders stipulate that the committee should be composed of no more than seven MPs, but the final number of members is determined each time by the Sejm. Candidates for members are nominated by parliamentary groups of at least 35 deputies. The final composition of the committee is approved by the Sejm in a joint vote. The Committee has a chairperson and two deputies that members elect.

In accordance with the Standing Orders of the Sejm, the scope of the Committees' activities is:

- Giving opinions on draft laws, decrees, orders and other normative acts concerning special services.
- Giving opinions on the directions of activities and examining annual reports of the heads of special services.
- Giving opinions on the draft state budget in the parts concerning special services.
- Discussing the annual report and other financial information of the special services.
- Giving opinions on proposals for the appointment and dismissal of candidates for the positions of heads of special services and their deputies; in the case of cba, this does not apply to deputy heads.
- Getting acquainted with the information from special services about particularly important development in their activities.
- Assessment of the cooperation of special services with other authorities, services and institutions authorized to perform operational activities for the protection of national security.
- Assessment particularly of the cooperation of special services with the armed forces, government administration bodies, law enforcement agencies and other state institutions as well as local government units, competent authorities and the special services of other countries.
- Evaluation of the protection of classified information.
- Handling complaints concerning the activities of the special services.
- Discussing information or reports on the activities of state institutions and bodies, other than the special services, obtained in the course of the special service's operational activities and preventive actions.

The effects of the work of the Committee, due to the secret nature of the issues discussed, are communicated to a very limited extent. On the website of the Sejm, the opinions of the Committee are available mainly around personnel matters (these opinions are not binding and do not contain any justifications). There are also draft amendments to laws, implementing regulations and internal orders relating to the activities of individual services (also non-binding). The Committee

issues recommendations (*desiderata*), but these are largely classified; only a list of them is made public. As a result, only a list of *desiderate* is published on the website. Plans for sittings are also published, containing a list of matters to be discussed. In the past, it was customary to publish reports on the activities of the SKSS, but in 2015 this ended. The Committee can also prepare a press release for the media about its sittings, but this has not happened since 2015.

Since its inception, the Committee has had a broad remit, and this remit has grown over time. However, in the execution of its tasks, the Committee is restricted by its quite modest powers. To date, no legislation has been passed to regulate its instruments of oversight. Similarly, no legislative act provides a comprehensive regulation of the duties of the Heads of special services *vis-à-vis* the Parliamentary Committee for Special Services. The Committee relies on information provided by the special services, and its role is limited to approving their actions. Since the very beginning of the Committee, it is the heads of the special services who decide which information to disclose or not. These discretionary decisions on their part are final and not subject to verification by their overseeing bodies: for instance, the President of the Council of Ministers or the Minister of National Defence. Ultimately, the scope of oversight is determined by the special services themselves.

A very serious weakness of the SKSS is the extremely limited auxiliary apparatus supporting the Committee's activities. In practice, the organizational base consists of a team of a few full-time administrative Sejm staff, whose task is to organize and handle sittings in a room guaranteeing the secrecy of meetings, keeping records and correspondence, running a registry. In addition to this modest administrative team the Commission has at its disposal a few occasional advisors. They are proposed by its members (one for each club delegating its members). These advisers, appointed in each Sejm term, although they are appointed by the Committee, in practice advise only the members of the parliamentary clubs that nominate them, so they are not advisors to the committee as a whole. Nor do they have any real independence, working exclusively for the representatives of the clubs that nominated them. The role of advisers is to provide substantive support to Committee members in preparation for sittings, in which they do not participate. Most often they are former officers of the services, mostly high-ranking officers, often former service heads.

In summary, the tasks of the Committee are defined quite broadly, giving theoretically the basis to expect a significant insight into the activities of the special services apparatus. The modest instruments granted to the Committee make this body a façade, lacking powers and opportunities for the proper execution of its mission.

3.1.8. Bodies appointed by the Sejm: Supreme Audit Office (NIK) and Ombudsperson (RPO)

3.1.8.1. NIK: Supreme Audit Office

The Supreme Audit Office or NIK (*Najwyższa Izba Kontroli)* is, in accordance with the Constitution, the principal state audit body, under the Sejm's control. NIK audits the activity of government administration bodies, the National Bank of Poland (NBP), state legal persons and other state organisational units with regard to legality, sound management, efficacy and integrity.

Among the state bodies subject to NIK control activities there are also the special services, as state administrative units. NIK carries out its activities with the special services as it does with other administrative units. Routine examinations include an annual assessment of the budget of the services in the framework of the audit of the state budget, in which it is contained. Reports from the conducted analysis are not published. In the course of control activities, NIK analyses the financial documentation of services, including classified ones, in terms of compliance of expenditure with the budget plan and legal provisions.

In addition, NIK carries out *ad hoc* audits of various aspects of the operation of special services, excluding operational-reconnaissance activities, that is key areas of their substantive mission activity. NIK's attention is therefore focused on organizational and legal issues, as well as on the management and coordination of their activities.

The achievements of NIK in relation to the special services and their supervisors are not extensive. But the findings made in the course of the few audits undertaken by NIK can be considered significant from the point of view of the conclusions upon the state of oversight of the special services.

The findings were contained in secret reports: the audit was provided to the most important persons in the state. Nevertheless, NIK has published press releases containing a summary of the most important findings and recommendations. Subsequent audits consistently indicated systemic deficiencies and dysfunctions in the organization and mechanisms of operation of the special services management model. To date, none of the critical comments have been taken up by governments. The recommendations have also not been implemented.

In conclusion, it should be noted that NIK, as the supreme state audit authority, has significant substantive potential to carry out thorough and reliable examinations on selected aspects of the activities of the special services. For this purpose, it has a professional audit methodology and qualified staff of employees

with specialist knowledge, experience and understanding of the issues of the special services, as well as high levels of security clearance.

The main difficulty limiting the ability to conduct in-depth and regular audits is that NIK must deal with the entire state and parts of local government. Subject-matter audits of special services, apart from the annual budget execution audit, may be carried out *ad hoc* at intervals of several years. Another issue, which is not systemic, is a very limited tendency (even reluctance) on the part of government administration to take into account the results of NIK audits. This problem does not only concern the special services.

The main obstacle undermining the effectiveness of NIK's audits of the special services is its limited access to information and documents concerning their substantive activities, particularly operational–reconnaissance work. Legal prohibitions and restrictions prevent the examination of precisely those areas where abuses most often occur, and which go to make up the core of the services' activities.

It should be added that the main prohibitions referred to by NIK are included in the provisions of the competence laws and the 2010 Act on the Protection of Classified Information. Provisions there directly cut off access to information on operational-reconnaissance activities, to anyone outside the services, with a very few exceptions related to criminal proceedings, when this access can be obtained by the court or the public prosecutor. The methods and forms of this work and the persons involved are not to be shared generally.

3.1.8.2. Commissioner of Human Rights (Ombudsperson)

The Commissioner of Human Rights, hereinafter RPO *(Rzecznik Praw Obywatelskich*) according to the Constitution 'upholds the freedoms and rights of the human and the citizen' set out in the legislation. The Commissioner is independent in his activities, and independent of other State organs. He or she is only accountable to the Sejm in accordance with principles specified by statute.

The RPO acts on its own initiative or at the request of citizens and their organisations. After reviewing the application, the RPO may take the case or transfer it according to its jurisdiction to another authority. Alternatively, they might indicate to the applicant what means of action he or she is entitled to.

The key competences of the RPO as an overseer towards the special services is their authority to apply to the Constitutional Tribunal on questions of whether laws or regulations issued by central state administration bodies comply with the Constitution. In addition, in criminal proceedings, the RPO may request the initiation of pre-trial proceedings in cases of offenses prosecuted *ex officio* and submit appeal measures, including emergency measures. The RPO can also participate in administrative proceedings, where they are entitled to apply for

the initiation of this procedure, lodge complaints with the administrative court, participate in any ongoing proceedings, carry appeals and legal questions to the Supreme Administrative Court. The same is true in civil proceedings.

In relation to special services, the role of the RPO is most often perceived in connection with the use of operational-reconnaissance activities. The RPO may request access to materials and information on the circumstances in which civil rights and freedoms were violated and request the services to provide findings and explanations on that issue. However, the restrictions indicated above mean that applications of this type are always subject to rejection from the services themselves.

3.1.9. Judicial oversight

3.1.9.1. The scope of judicial power over special services

Judicial oversight of the special services is extensive and includes both the common judiciary, the administrative judiciary and the Constitutional Tribunal.

The scope of the common judiciary includes operational-reconnaissance activities, including mainly the authorization of applications for: operational control; the use of information constituting banking and financial secrecy by services; and the control of telecommunications data. The court competent to examine the applications of authorized services is the District Court in Warsaw.

The administrative judiciary exercises oversight over:

- Administrative decisions issued by the heads of the special services as government administration units, typically with regards to the staff of these services, for example the decision to release a member from service.
- Decisions of the state security services (ABW and SKW) towards citizens regarding the protection of classified information. This might be, for instance, decisions refusing to issue a personnel security clearance; or a decision to withdraw a security certificate.

The competent courts in the case of the control of decisions of the special services are the Voivodship Administrative Court in Warsaw (first instance) and the Supreme Administrative Court in Warsaw.

The Constitutional Tribunal's jurisdiction towards special services consists in examining the compliance of the provisions of the generally applicable law regulating their functioning with the Constitution.

3.1.9.2. Constitutional Tribunal

Over the past 35 years, the Constitutional Tribunal has issued a dozen or so rulings on the activities of the special services, including a few of major importance, significantly affecting legislation in this area.

The most important decisions concerning the special services include judgments on the powers for the use of operational-exploratory activities. In particular, there has been the judgment of July 2014 on regulations specifying powers for the use of operational control. The Tribunal formulated a number of precise guidelines regarding the principles for formulating powers for special and law enforcement services in the Acts for the use of technical means for the secret acquisition of information. It pointed out that the catalogue of types of these measures must be closed, in order to limit the arbitrariness of state authorities and to exercise effective control over secret operational and reconnaissance activities. However, the so-called surveillance laws adopted in the implementation of the judgment by the parliament did not take this guideline into account. Indeed, parliament increased the powers of the services, without introducing an oversight and control mechanism. These irregularities indicated, among others, Venice Commission in its opinion of June 2016.

3.1.9.3. Judicial oversight of operational – reconnaissance activities

Since 2002, judicial oversight has included the use by special services of 'operational control'. In accordance with the provisions of the competence laws (regulating this issue in the same way for each of the authorized services), the court orders the use of 'operational control when other measures have proved ineffective or are likely to be ineffective or useless'.

Operational control is decreed by the court at the request of the head of the service, after obtaining the consent of the First Deputy Prosecutor General-National Public Prosecutor (hereinafter the National Public Prosecutor). The competent court in the case of the special services, as indicated above, is the District Court in Warsaw. A given act of control is ordered for not longer than three months, with the possibility of a one-time extension for a further three months. The procedure does not provide for ongoing or follow-up control of the measure and its effects, including an assessment of the purpose and suitability of its use. The only exception is when the control is subject to an extension, since the request for extension must include an explanation of why the control has not ceased.

In urgent cases, where there is a danger of the loss of information or the obliteration or destruction of the evidence, the head of the ABW (CBA, SKW) may order, upon the consent of the National Public Prosecutor, operational control. The ABW head simultaneously submits a request to the court to issue a decision to this effect. The court is to issue a decision within five days. When consent has not been

obtained from the court, the service head suspends operational control and orders the immediate destruction, by protocol in the presence of a commission, of the evidence gathered in the course of the operation.

The District Court in Warsaw also exercises oversight in relation to the acquisition by the services of telecommunications, internet and postal data. This oversight consists in the court receiving periodic reports from the services (every six months) covering the number of cases of obtaining telecommunications, internet and postal data during the reporting period and the type of these data, together with an indication of the crimes related to the cases in which these data were obtained. At the same time, the services are required to keep records of requests for the data in question. The above periodic reports are the only form of review by the court of the said activities of the services. The services are not subject to any individual form of control, authorisation or individual follow-up control. We are dealing only with quantitative control, and, it seems, that the court does not verify the legitimacy of the data collected.

Another element of judicial oversight is the oversight of the acquisition of financial data at the request of the ABW or the CBA. In situations where it is necessary to effectively prevent crimes specified in the statutory catalogue, ABW and CBA may use secret information processed by banks. The consent for access to these data is issued by the District Court in Warsaw, at the request of the head of the service. After obtaining consent, the service informs in writing the entity obliged to provide information. A refusal by the court may be appealed by means of a complaint.

These two types of judicial oversight: surveillance and the use of telecommunication, internet, and postal data, have one thing in common. In both cases, the legislators failed to secure permanent organizational structures within the court framework to pursue this kind of activity. Additionally, they failed to provide additional funding and personnel for the purpose. As a result, courts cannot appoint judges whose primary activity would be to oversee surveillance activities. Such judges would be able to specialize around the question and could rely on the suitable auxiliary (administrative) apparatus. Given the sheer scale of surveillance activities, suitable administrative structures for the purpose of permanent oversight would be justified. Other forms and means of operational – reconnaissance work, discussed in point (3) above, remain outside the oversight of the courts.

3.1.9.4. Administrative courts

The administrative court plays a control role in two types of situations. First, when the services, which are central state administrative units, issue administrative decisions, these are subject to the review of administrative courts on general principles. Most often, these decisions concern officers and employees, because the service relation of officers is regulated by the Code of Administrative Procedure. All decisions of the heads of the special services concerning the course and

conditions of the service and remuneration or other benefits are challenged in the ordinary course of things before the administrative court.

Administrative courts are empowered to examine complaints about the actions of public administration, including, in the field of service oversight, different areas of their activity.

The second type of control of the administrative court is the handling of the complaints of citizens against the decisions of the ABW and the SCW regarding the protection of classified information, i.e., a decision to refuse to issue a personal security certificate or to withdraw a security certificate. This procedure is also subject to control decisions of other heads of special services (AW, SWW, CBA) issued in relation to their own officers, against whom they perform the functions of state protection services.

A person dissatisfied with the decision of the head of one of the services is entitled (after exhausting the appeal route to the Prime Minister) to make a complaint to the Voivodeship Administrative Court in Warsaw. This checks the legality of the decision made in administrative proceedings.

3.1.10. Conclusion

The oversight and control set up in Poland over the special services is not a coherent system. Nor is it a consciously created functional and institutional model, established by a unified legal act to achieve specific goals and needs of the state. Its dominant feature is the limited or vague scope of tasks of individual state authorities in the evaluation of the activities of the services. These do not adequately specify the mandate of these bodies and the adequate tools for its implementation. As a result, most key areas remain effectively impervious to external evaluation.

The view of oversight and control authorities, in particular those external to the administration, is fragmented and covers only certain aspects of the activities of the special services. However, even in these cases, the limited scope of access to documents and information makes the assessments superficial, unprofessional and often even amateurish. An important weakness is also what we might call *ad hoc*ness (even spontaneity), reactivity and fragmentation of oversight and control, often carried out under the dictation of political life events or because of emerging scandals.

However, the main weakness of the Polish model remains the scanty instrumentation (competencies), primarily due to statutory restrictions on access to the most sensitive (important) information illustrating the substantive activities of the services. In addition to the regulations contained in the competence laws, the main obstacle is the current system of the protection of classified information.

In practice, this system prevents effective oversight not only of the legality of the special services' activities, but also of their purposefulness, reliability, efficiency, and effectiveness. The principles on which it operates mean that none of the said oversight and control entities has access to information that allows them to independently assess the manner in which the special services perform their tasks. As a result, the oversight and control authorities, in carrying out their tasks, have access only to the information and documents that the heads of services decide to make available to them. This means that they are not realistically able to conduct independent control proceedings or to formulate standalone, objective and independent assessments on their basis.

A serious deficit is also the lack of a body dedicated to dealing with citizens' complaints about the activities of special services. This would require a statutory, strong mandate authorizing independent investigations with access to all documents and information necessary for assessing the legitimacy of the complaint.

The scope of tasks and the powers of the oversight and control authorities leave the activities of the services beyond real substantive control. None of the bodies is to have any formal or factual competence to objectively and reliably assess the purpose, efficiency and effectiveness of the operational activities carried out.

Lack of mechanisms and tools to assess the suitability and quality of the tasks performed, extends to the administrative government, parliament, and to public opinion. Largely absent from public debate is the issue of the effectiveness of public funds spent on the activities of special services, and the question of whether the scale of these expenditures is justified.

The effects of oversight and control bodies are therefore unreliable, and knowledge and assessments do not objectively reflect the actual situation. The image of the activities of the services that reach political decision-makers, parliament, the judiciary and society is deformed, fragmentary and shaped largely in accordance with the will and interests of the services themselves.

In summary, the mandates and powers of the special services control and oversight authorities are too limited and leave out large, important areas of substantive activity of the services (operational activity), and the tools they have to perform their functions. This includes access to information and documents. This means that the most sensitive areas of activity are not actually reached. Moreover, the practice developed over the years largely limits the view and awareness of imperfections in the services, sanctioning a widespread belief that there is no alternative, and thus significantly reducing innovative initiatives to break the deadlock.

3.2. Croatian case study: Intelligence and law enforcement mandates/powers

Dragan Lozancic

3.2.1. Introduction

Croatia's intelligence community was built on the foundations of a failed ideology, a decoupling federation, democratic aspirations, political crisis, and war. There would be turbulence from the outset of Croatia's independence from the former Yugoslavia in 1991. Setting up a successor to a service notorious for its repressive and brutal ways proved highly contentious. As an existential threat loomed large, national unity would trump calls for lustration.[306] It was a time for difficult compromises. There was little choice but to rely on experienced ex-Yugoslav officials and security service operatives in the early 1990s. As a result, Croatia's first domestic intelligence service SZUP was not unlike the SDS, its Yugoslav predecessor. Based out of the Interior Ministry of a newly elected democratic government, SZUP retained all the hallmarks of communist-era secret police, including its enforcement powers. It would play an important role in defending Croatia's constitutional order, as well as in counterinsurgency (counterespionage) during the war. But accusations of abuse, human rights violations, and politicization would chip away at its reputation. Public trust eroded away, and the reputation of the intelligence community as a whole suffered.

Today, the Security and Intelligence Agency (SOA) is Croatia's civilian domestic and foreign intelligence service. SOA is an integral cog in Croatia's national security structures. It provides important support to policy – and decision-makers in promoting and safeguarding national interests, both at home and abroad. While high crimes, transnational criminal groups, and complex corruption schemes are not exactly outside its purview, SOA does not have a law enforcement mandate or police powers. Cooperation with the police and state prosecutors is cordial, though inherently tempestuous, as each pursues its own institutional interests. As Croatia is a member of the European Union (EU) and the North Atlantic Treaty Organization (NATO), SOA maintains a robust network of bilateral partnerships and is itself a member of key multilateral intelligence cooperation initiatives across the Euro-Atlantic. Its former

306 Croatia was one of several post-authoritarian societies in Europe that decided not to enact lustration, an equally contentious concept in liberal democracies irrespective of whether adopted or not. As a matter of transitional justice, lustration implies vetting individuals from public institutions that were associated with past authoritarian regimes, often directly suspected of being involved in human rights abuses, collaborating with authoritarian regimes, or taking part in other misconduct. Unlike other Central and East European countries in transition, Croatia faced an existential threat that required national unity. However, many years after the conflict ended, calls for lustration would frequently resurface in political discourse.

director Daniel Markić is now head of INTCEN, the closest thing to an EU intelligence service.[307] SOA's road to reform, impressive but far from ideal, could provide important lessons well beyond its regional reach.

3.2.2. Background

Croatia was one of six former republics to emerge as an independent state from the break-up of the former Yugoslavia. As one of the founding members of the non-aligned movement, Yugoslavia had international respect and influence despite its communist pedigree. It seemed to be cunningly outmanoeuvring the vying great Cold War powers and bipolar rivalries. It stood up to Stalin and resisted pressure to join the Warsaw Pact. It would also rebuff NATO and stay out of Western European integration. Eventually, it established friendly ties to both the former Soviet Union and the United States. Its non-Soviet styled, alternative brand of communism and its East-West buffer-zone status got it access to many Western countries. But one should have no doubts about the former Yugoslavia's repressive and authoritarian system of governance. As such, its one-party rule greatly relied on the intimidating and coercive exploits of the State Security Service (SDS).

The SDS, still best known by its earlier acronym UDBA, was the former Yugoslavia's domestic intelligence service, though it was equally adept at conducting clandestine operations abroad as it was at home. Perceptions of its prowess—often unsubstantiated or controversial and sometimes based on stereotypes and myths—varied.[308] Some talked of incompetence, others claimed that UDBA had influence in all aspects of social, economic, and political life in the country.[309] The SDS had its central federal headquarters in Belgrade and semi-autonomous branches in each of the Yugoslav republics. It served to protect the state against both foreign and domestic enemies, real or otherwise. It was relentless and brutal in the pursuit of its mission. Ruthless criminals were often recruited to do its 'dirty work' in kidnapping and murdering dissidents and activists. During the Cold War, the security services were suspected of being behind over 70 murders of Yugoslav emigres in Western countries,[310] with at least 29 killings allegedly committed in Germany alone.[311] At home, the SDS's exceptional law enforcement powers often served as leverage to intimidate and exert collaboration

307 Pinto, N.T., 2025. 'We know what Russia is doing and how it does it, EU intelligence centre chief tells Euronews'. Euronews (interview), 25 May. Available at: https://www.euronews.com/my-europe/2025/05/23/we-know-what-russia-is-doing-and-how-it-does-it-eu-intelligence-centre-chief-tells-euron [Accessed 25 May 2025].

308 Krašić, W., 2018. 'Služba državne sigurnosti Socijalističke Republike Hrvatske potkraj 1970-ih i početkom 1980-ih' ('The State Security Service of the Socialist Republic of Croatia at the end of the 1970s and early 1980s'). *Zbornik Janković*, 3/3, 355–387 at 356.

309 Krašić, W., 2018. 'Služba državne sigurnosti'.

310 AP, 2008. 'Ex-spy tells of killings'. *Associated Press*, 3 October.

311 Hofmann, F., 2014. 'Yugoslav spy trial in Munich'. Deutsche Welle, 17 October. Available at: https://www.dw.com/en/former-yugoslav-spies-on-trial-in-munich/a-18000914 [Accessed 20 May 2025].

or information. Towards the time of Yugoslavia's break up, it had accumulated a vast network of informants (collaborators) and hundreds of thousands of files on its own citizens. The mere mention of the Service would send shudders down a citizen's spine.

The fall of the Berlin wall and a looming political crisis in the former Yugoslavia were clear enough signs for Croatia's SDS operatives. It was clear that tectonic changes were coming. Croatia's first free, multiparty elections brought in a new democratic government in 1990 and a referendum on independence. The overwhelming public support for an independent Croatia convinced many security officials to throw in their lot with the new political elites. And when ethnic Serbs in Croatia raised an armed rebellion—much of it orchestrated through covert Yugoslav intelligence operations and with full support of the Yugoslav army—most SDS operatives in Croatia felt they had little choice. At the time, ethnic Serbs made up about 12% of Croatia's population and 29% of the SDS total workforce in Croatia.[312] After years of ideological indoctrination and uneven multiethnic make-up in Yugoslav institutions, (Croatian) national sentiments, trust, and loyalty would be the key screening factors in retaining experienced agents.

3.2.3. Building a new intelligence foundation

The building blocks of Croatia's intelligence structures, just as its armed forces, had to be forged from scratch and in the most trying circumstances, during the 'Homeland War' (1991-1995). Analysts have argued that Croatia's intelligence community was not a successor of any previous system whatsoever.[313] It was unlike another former Yugoslav republic, neighbour Serbia, whose intelligence service BIA proudly claimed a security service tradition dating back to 1899.[314] But like other Yugoslav republics, Croatia did inherit much of the fragmented manpower, infrastructure, and vast databases in its possession. The dual effects of emerging from an authoritarian system and almost immediately having to defend Croatia's sovereignty in a violent armed conflict had a direct impact on how intelligence was organized and how it would develop.[315] The Office for the Protection of Constitutional Order (SZUP) was established within Croatia's new Interior Ministry, along the same lines as its SDS predecessor. It was set up as an enforcement body alongside the regular police, sharing the same investigative and coercive powers.

312 Akrap, G. and Tuđman, M., 2013. 'From totalitarian to democratic intelligence community – case of Croatia (1990–2014)'. *National Security and the Future* 14/2, 74–132 at 95; Lučič, I., 2023. 'Hrvatska izvještajna služba u obrani Republike Hrvatske' ('The Foreign Intelligence Service in the Defense of Croatia'). In: Ž. Holjevac et al., eds. *Miroslav Tuđman i paradigm znanja*. Zagreb: Udruga sv. Jurja, 345–365 at 346.

313 Akrap and Tuđman, 2013. 'From totalitarian', 77.

314 BIA – Security-Intelligence Service, 2019. 'The speech of the Director of the Security Information Agency, Mr. Bratislav Gašić, BIA Anniversary 2019'. *Republic of Serbia*. Available at: https://www.bia.gov.rs/en/media/public-statements/the-speech-of-the-director-of-the-security-information-agency-mr-0/ [Accessed 25 January 2025].

315 Cvrtila, V., 2013. 'Razvoj i nadzor sigurnosno-obavještajnog sustava u Republici Hrvatskoj' ('Development and Oversight of the Security-Intelligence System in Croatia'). DCAF, 3.

The new service was mostly staffed with experienced ('old guard') operatives and some new recruits, many with a police or criminology background.

SUZP's role was to protect the constitutional order, mainly by uncovering and preventing threats to state security. It was a vaguely framed mission with latitude for flexible interpretations, further enshrouded in highly classified executive-order bylaws. Its secret surveillance and communication interception measures were approved by the Interior Minister, who was obliged to immediately inform the President of such measures. The President exercised executive powers over intelligence. A 'paper tiger' oversight commission was also established, giving the impression of genuine supervision over SUZP and respect for individual rights and freedoms. The new government was more concerned, though, with defending the country's sovereignty and territorial integrity, than it was about instilling democratic governance standards in the security sector: especially so after losing a third of the national territory. Under such trying circumstances and not having yet fully experienced the benefits of living in a free society, people were, by and large, more likely willing to cede their newly acquired individual liberties for greater security.

The role of Croatian intelligence in the war was monumental. Croatia would establish other fundamental intelligence bodies like defence/military intelligence services and a foreign intelligence service (OU/HIS), as well as an executive hierarchy for coordinating and managing intelligence efforts.[316] Counter-intelligence was particularly instrumental in thwarting and exposing Yugoslav sponsored subversion, as in operation 'Labrador,'[317] Serbia's attempt to portray Croats and its government as fascist and anti-Semitic.[318] Such efforts were intended to suggest the revival of a World War II Nazi-aligned puppet government, ignoring or downplaying the role of Croatia's then president in Yugoslavia's anti-fascist resistance during the war.[319] The conflict would end following a successful military offensive in 1995 and helped regain most of Croatia's lost territory and a follow-on peaceful repatriation of a strip of its territory in the East. The post-war period would see the further development of intelligence structures and capabilities, but little to nothing was done to strengthen intelligence governance standards, nor was oversight and accountability very high on the agenda.

SZUP's reputation, despite its important counterintelligence role during the war, would deteriorate through the decade. This was notwithstanding Croatia's genuine

316 Tuđman, M., 2000. 'The first five years of the Croatian Intelligence Service: 1993–1998'. *National Security and the Future* 1/2, 47–74.

317 On 19 August, 1991, Yugoslav army intelligence operatives planted and detonated two explosive devices at a Jewish community centre and Jewish cemetery in Zagreb. Operation 'Labrador' was a false-flag covert action and part of a wider Serb effort to defame Croatia's struggle for independence and manipulate Croatia's internal cohesion (especially aimed at its ethnic Serb population).

318 Perković Paloš, A., 2024. 'Attempts of defamation of Croatia as antisemitic in the 1990s: False flag operation Labrador'.
Review of Croatian History 20/1, 115–138. Available at: https://hrcak.srce.hr/file/468709 [Accessed 11 May 2025], 115-116.

319 From today's perspective, it is strikingly comparable to Russia's propaganda portraying Ukraine's government, despite being led by a Jewish president, as being dominated by neo-Nazis.

security concerns, including significant international pressures on its domestic and foreign policies.[320] There was a sizable UN peacekeeping mission in Croatia and next-door in Bosnia and Herzegovina (later a NATO and then EU mission). Croatia and its southeast neighbourhood was a hotbed of local and external factions vying for competing interests. By many accounts, SUZP may not have been up to the task. Its widespread targeting of journalists, activists, and political opponents reflected its recklessness, ineptitude, or malice in failing to distinguish between legitimate criticism and political opposition to government, on the one hand, and the subversion of national security, on the other. It was not fully trusted by its own government elites, writes one analyst, adding that it had struggled in securing convictions in the criminal cases it brought forward to prosecution.[321] Nevertheless, SUZP was able to dominate the intelligence community with its sheer size and authority, not to mention its enforcement powers. But two reform efforts in 2002 and 2006 would fundamentally reshape Croatia's intelligence community.

Croatia's Euro-Atlantic ambitions gained momentum in the early 2000s. A new coalition government—more fully committed to Euro-Atlantic integration—was also keen on embarking on intelligence reforms. War in the 1990s and international criticism of post-war government policies had put Croatia well behind other East European countries in terms of EU and NATO membership. At about the same time, the Venice Commission, the Council of Europe's Parliamentary Assembly, and European court rulings (mostly involving human rights and national security) were contributing to a growing body of standards for governing security services in democracies. This would have a direct impact on Croatia's intelligence reforms and how SUZP's law enforcement status and mandate would fundamentally change.[322]

The intelligence services would also feature in Croatia's amending the constitution in 2000. There was a consensus that Croatia's semi-presidential system of governance should be shifted closer to parliamentary democracy. The reforms essentially transferred most executive powers to a parliamentary government, headed by a Prime Minister. The amendments (today Articles 81 and 103 of the Constitution) specifically mentioned the 'security services', a term which directly applies to intelligence bodies as indicated by Smerdel.[323] In effect, it resulted in establishing an executive power sharing scheme between the Croatian President and Prime Minister. It would also empower the parliament's oversight authority for the intelligence services. From now on, the President and the Prime Minister's government would jointly guide the work of the intelligence services. The heads of

320 International actors would be highly critical of Croatia's minority rights track record, its policy towards neighboring Bosnia and Herzegovina, and its lack of full cooperation with the International Criminal Tribunal for the former Yugoslavia (ICTY) in the Hague, Netherlands.

321 Lefebvre, S., 2012. 'Croatia and the Development of a Democratic Intelligence System (1990–2010)'. *Democracy and Security* 8/2, 115–163, 125.

322 Cvrtila, 2013. 'Razvoj', 12.

323 Smerdel, B., 2014. 'Republic of Croatia'. In: L. Besselink et al., eds. *Constitutional Law of the EU Member States*. Deventer: Kluwer, 191–247 at 236.

intelligence services would have to be jointly appointed by the President and Prime Minister. Although not binding, a parliamentary committee would also provide an opinion on a candidate before his or her appointment.[324]

In 2002, new legislation (Law on the Republic of Croatia Security Services) would set the stage for Croatia's most extensive post-war intelligence reconstruction. It was the first time that all the key elements of Croatia's intelligence community were brought together under a single statutory banner.[325] SZUP would be transformed into a new counterintelligence agency (POA) and would no longer have law enforcement powers. Nor would it be part of the Interior Ministry. However, POA would still retain the state's telecommunication interception centre (used by both POA and police authorities). Croatia had, after these reforms, three intelligence services: foreign (OA), domestic (POA), and military (VOA). A National Security Council (VNS) and a coordination body would also be established, as well as parliamentary and independent civilian oversight committees. Setting up an intelligence oversight committee consisting of ordinary citizens was as audacious as it was experimental.

The new law also established that the National Security Council would adopt annual intelligence guidance (intelligence priorities), a clause still relevant today. In July 2003, the Council adopted its first intelligence guidance. It was unclassified and openly available to the public.[326] It would also be the last time, as all subsequent intelligence guidance documents would not be made publicly available. The 2003 guidance does, however, make it clear that organized and economic crime would be among the many intelligence tasks, albeit they would be more narrowly defined. It outlines how the 'agencies will continue investigating more complex forms of crime' which are characterized as being exceptionally organized, highly secretive, sophisticated, and transnational.[327] But it also makes clear that once the intelligence work is done, enforcement and prosecution would be a matter entirely left to other bodies. Current intelligence guidelines have unclassified and classified parts. Why the unclassified part has not been shared with the public remains elusive. But given that SOA has been publishing annual public reports since 2014, it is possible to get some sense of Croatia's intelligence priorities in the last years.

324 The parliamentary intelligence oversight committee would invite a candidate to appear at a closed hearing session and ask them to answer questions from its members, after which the committee would vote on a conclusion. While much of the content in the hearings are classified, the committee usually informs the public of its general conclusions. Although the committee's opinion is non-binding on executive decisions to appoint intelligence directors, anything short of the committee's bi-partisan consensual support would certainly weigh on a candidate's perceived legitimacy once appointed. Over the years, Croatia has experienced both unanimity in committee support and bi-partisan bickering in reaching split opinions on candidates.

325 NN (Narodne Novine/Official Gazette), 2002. *Zakon o sigurnosnim službama Republike Hrvatske* (The Law on the Republic of Croatia Security Services), 32/02, 38/02.

326 NN (Narodne Novine/Official Gazette), 2003. *Godišnje smjernice za rad sigurnosnih službi Republike Hrvatske* (Annual guidance for the Republic of Croatia Security Services), NN 121/2003 (29 July).

327 NN (Narodne Novine/Official Gazette), 2003. *Godišnje smjernice.*

Although the new domestic intelligence service no longer had enforcement powers, it apparently had not shed old mindsets. POA would find itself publicly implicated in a high-profile 2004 incident involving a young journalist. Its agents were accused of luring the journalist under false pretences, unjustified detention, and intimidation (to become an informant). It would not only expose improper conduct of POA's operatives, but perhaps even more worrisome, it resulted in a complete meltdown of newly established oversight functions. The chairman of the new civilian oversight committee, a respected academic figure, resigned in protest. Even though the head of the service was eventually removed and several agents reprimanded, the affair reflected badly on the agency's already tarnished reputation and followed a familiar pattern that continued to further erode public trust. The affair resonated in Brussels as an EU report on Croatia's progress towards membership concluded that there may be grounds to believe human rights were violated, and that there had been 'no specific follow-up' in the case, questioning Croatia's ability to exercise effective intelligence oversight.[328] The young journalist would have to wait ten years for compensation after winning a civil lawsuit in 2014.

It was more likely that pressure from Brussels, rather than a genuine desire for reforms, ushered in the second major restructuring of the intelligence community in 2006. The Law on the security-intelligence system of the Republic of Croatia united the foreign and domestic intelligence agencies into a single civilian security intelligence service SOA.[329] By merging foreign and domestic intelligence, SOA is a model that only a dozen or so European countries have adopted. It would strictly be an intelligence service and would not have police powers or a law enforcement mandate. There were reports of a last-ditch effort to bring back police powers before the law was adopted, but it was eventually discarded.[330] While any substantial discussions took place behind closed doors, a formal explanation of the new law was submitted to the Croatian parliament. Among the reasons given for merging the former services together was difficulty in delineating between internal and external threats, with emphasis on transnational organized crime and terrorism.[331] For a small country like Croatia, it was argued, having a single civilian intelligence service seemed sensible.

The foreign intelligence service was still reeling from a period of instability in the late 1990s when its directors were removed and several senior agents were brought in for questioning by the police.[332] In the early 2000s, the police would be

328 European Commission, 2005. *Croatia 2005 Progress Report*, SEC(2005) 1424, Brussels, 9 November, 13-14.

329 NN (Narodne Novine/Official Gazette), 2006. *Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske* (The Law on the security-intelligence system of the Republic of Croatia), NN 79/06, 105/06.

330 Lefebvre, 2012. 'Croatia', 138-139.

331 Government of Croatia, 2022. 'Božinović: MUP zbog lažnih dojava surađuje sa SOA-om, Interpolom i Europolom' ('Božinović: due to bomb threats, Interior Ministry is cooperating with SOA, Interpol and Europol'), 20 June. Available at: https://vlada.gov.hr/vijesti/bozinovic-mup-zbog-laznih-dojava-suradjuje-sa-soa-om-interpolom-i-europolom/35624 [Accessed 20 May 2025], 41-42.

332 Lučič, I., 2023. 'Hrvatska', 361.

called in to intervene, once again under extraordinary conditions.[333] It is no wonder the foreign intelligence service reportedly resisted, to no avail, the merger with POA, its much larger and politically more influential sister service. It would prove to be a traumatic experience for many. The merger itself resembled a corporate-like hostile takeover, as POA was able to quickly exert its dominance when the organizational cultures of the two clashed. Staff from POA would also fill key leadership posts in the new service. It would take many years before SOA would shape its own organizational culture.

The new law also clearly outlined the extensive mandates of three separate oversight bodies: parliamentary committee, executive body, and civilian committee. Two measures would affect oversight. First, a member of parliament from the main opposition party must preside over the parliamentary committee. Second, a newly established body, UVNS, would also be mandated to oversee intelligence. UVNS would be an arm of the executive, but could investigate cases (complaints), too, on behalf of parliament. A new national telecommunication interception centre OTC was established as a separate organization (previously situated in the counterintelligence agency POA). Numerous best practice standards and safeguards were introduced to protect against the abuse of special powers.[334]

Effective intelligence oversight struggled in Croatia. Neither did the new Agency, SOA, quickly earn public trust. Several incidents would require its main watchdog, the opposition-chaired, bipartisan parliamentary intelligence oversight committee to investigate.[335] In 2014, a scandal erupted when media reports revealed suspected discriminatory hiring practices in earlier years. The committee immediately opened an inquiry. Unfortunately, members of the committee were unable to overcome their partisanship differences and reach a common conclusion. They would also selectively leak self-serving information to the press. Like any other part of the public sector, intelligence itself had become a political battleground, and the oversight body was just another forum for competing narratives between the governing coalition and opposition parties. This was especially so when partisan interests were at stake. Even senior parliamentarians seemed to be inept at balancing their committee responsibilities (duties) and political party loyalties. It is not an uncommon challenge. Intelligence oversight in the US Congress, writes Gregory McCarthy, 'has gone from partisanship to hyperpartisanship to intermittent dysfunction'.[336]

333 Akrap and Tuđman, 2013. 'From totalitarian', 115.

334 For a good account of the new changes and its shortfalls, see Cvrtila, V., 2013. 'Razvoj', 17-22; and for a detailed description of SOA's legal framework and mandate, see Markić, D., 2002. 'Chapter IV Croatia'. In: P. Burczaniuk, ed. *Legal Aspects of the European Intelligence Services' Activities*. Warsaw: Internal Security Agency (Poland), 49–64.

335 Lozančić, D., 2020. 'Insights and Lessons Learned from Croatia's Intelligence Reforms'. Geneva: DCAF, 20 November. Available at: https://www.dcaf.ch/insights-and-lessons-learned-croatias-intelligence-reforms [Accessed 22 March 2025], 6 and 13.

336 McCarthy, G.C., 2024. 'When Oversight Went Awry: Congress and Intelligence in the Twenty-First Century'. *International Journal of Intelligence and CounterIntelligence* 37/3, 1022–1055 at 1022.

The politicization of intelligence continued to be an ever-present danger. Releasing accurate but incomplete intelligence information or cherry-picking what to release or misrepresenting intelligence information to stake a political position are egregious forms of politicization.[337] After a recent political bout between executive and legislative bodies over the use of intelligence information, Croatian award winning journalist Nataša Božić was highly critical of political elites, warning them that what they were doing was 'irresponsible and dangerous,' adding that a lot of effort has been invested over the past fifteen years to professionalize and depoliticize SOA in reaching high professional standards.[338] If an intelligence agency 'ever loses its reputation for objectivity, nonpartisanship, and professionalism,' argue Zegart and Morell, 'it will lose its value to the nation'.[339]

Recent media reports and independent commentators attest that confidence in SOA's integrity and utility has been slowly but gradually growing. Just over a decade ago, media coverage was almost exclusively critical, often uncovering misdeeds. The oversight committee had rarely been able to reach any meaningful consensus in its supervision of SOA. In February 2025, the committee was unanimous in praising SOA's work at a closed hearing. And this was not the only time. It has become a familiar pattern as of late. The decision to separate law enforcement from SOA's domestic intelligence efforts may finally be paying off for Croatia. Or, it might also be that the three-tier intelligence oversight bodies have come of age, suggesting supervisory authorities have steered the Agency down a more mission-focused, law-abiding path. Or, it might just be a result of a new generation of leaders. Whatever it is, the Agency has apparently opened a new chapter, well away from the controversies that marked its earlier years.

3.2.4. Current state of play: Intelligencel-law enforcement nexus

In Article 23 of the current law,[340] SOA's functional role is twofold: (1) assure domestic security; and (2) provide foreign intelligence. The first reflects SOA's inherited counterintelligence function (confined to activities on Croatian territory), so often the target of much of the criticism in the past. It emphasizes a 'preventive' posture aimed at threats to Croatia's constitutional order, state authorities (bodies), its citizens, and national interests. The second function is outward focused and

337 Gioe, D.V. and Morell, M.J., 2024. 'Spy and Tell: The Promise and Peril of Disclosing Intelligence for Strategic Advantage'. *Foreign Affairs*, 23 April.

338 Božić, N., 2024. 'TNT komentar: Zloporaba SOA-e u stranačke svrhe – to nije novi običaj nego stara navada' ('Commentary: abusing SOA for political party purposes is not a new custom but an old habit'). N1, 20 October. Available at: https://n1info.hr/n1-komentar/tnt-komentar-zloporaba-soa-e-u-stranacke-svrhe/ [Accessed 11 April 2025].

339 Zegart, A. and Morell, M., 2019. 'Spies, Lies, and Algorithms: Why US Intelligence Agencies Must Adapt or Fail'. *Foreign Affairs*, May/June.

340 NN (Narodne Novine/Official Gazette), 2006. *Zakon.*

serves to help Croatia's authorities understand what is going on in the world and what to do about it. But while the 2006 law was able to force the merger of two intelligence agencies (foreign/domestic) into one organization, its authors were unable to articulate the new agency's role in a single paragraph. To its credit, SOA was able to come up with a simple, unified mission statement:

> *We detect, investigate and understand security threats and challenges by collecting and analysing intelligence significant for national security, thus providing the state leadership and other state bodies with reliable intelligence support in decision-making and act to protect Croatia's national security, interests and the well-being of its citizens.*[341]

Nevertheless, Article 23 of the current law[342] specifically highlights several concerns the Agency should be particularly attentive to: terrorism; espionage; violent extremism; threats to senior government officials; organized and economic crime; threats to information and communication networks (ICT critical infrastructure); unauthorized disclosure of classified information; and 'other activities' that might endanger national security. The last is a 'catch-all phrase' since there is no definition of national security in Croatia's legal framework. If the law had been written today there would also have been: hybrid threats; cyberattacks; disruptive technologies; and misinformation (influence campaigns, especially in national elections).

Much of law enforcement in Croatia falls on the shoulders of its national police force, with headquarters in Zagreb and regional police stations throughout the country. It is part of the Ministry of Interior and has specialized units for organized crime and corruption, illicit trafficking, border security, cybercrime, and countering terrorism, as well as a tactical anti-terrorism unit. The State Attorney's Office (DORH) is an independent and autonomous judicial body responsible for criminal prosecutions. It has a specialized unit USKOK responsible for investigating and prosecuting corruption and organized crime. Both police investigators and USKOK are authorized to use special evidentiary measures, as outlined in Articles 332-340 of the Criminal Procedure Code (i.e. secret surveillance, communication intercepts, house searches, and undercover agents). Although these measures are not unlike the special measures used by SOA, there are procedural and other differences, including in how warrants are issued. For example, while police requests for communication intercepts are handled by regional and lower court judges, all intelligence warrants of SOA have to be approved by specially appointed Supreme Court judges. Other bodies and organizations also provide support (i.e. financial expertise).[343] This represents much of the bulwark of Croatia's law enforcement community.

341 SOA – Security Intelligence Agency, 2023. *Public Report 2022*. Zagreb: SOA.

342 NN (Narodne Novine/Official Gazette), 2006. *Zakon*.

343 The Independent Sector for Financial Investigations and the Anti-Money Laundering Office are just two examples.

Croatia's Criminal Code, under Chapter 32 Criminal Offenses Against the State, Articles 340-351, provides a natural foundation where intelligence and law enforcement interests overlap. High treason, subversion, espionage, attacks on the most senior government officials, and disclosure of classified information are among the punishable offenses that also endanger national security. Prosecutions are rare indeed. In many countries, such acts are also referred to as 'state' or 'national security' crimes. A separate section in the Criminal Code on terrorism (Articles 97-102) and government counterterrorism strategies represent a strong basis for both intelligence and law enforcement bodies to closely cooperate. Terrorism is one of the many threats both have to deal with. It is also a threat, where working together, can be mutually beneficial. SOA's ability to act in preventive fashion enables it to accumulate valuable information, well before the police have any indication of a possible suspect, much less reached 'probable cause' and/or 'reasonable suspicion' thresholds to take action.

The 'symbiotic relationships' analogy is as good a paradigm as any to reflect the real-life interactions of SOA and Croatia's law enforcement bodies. It is probably similar in many other countries as well. In almost any given case, their interests can easily converge, diverge, or be indifferent to one another's concerns. Ideally, both can benefit from cooperation (*mutualism*). But just as easily, one can benefit at the expense of the other (*parasitism*). For example, the police and prosecutor might want to arrest suspects sooner rather than later in a particular case, perhaps fearing perpetrators might evade justice by fleeing or destroying evidence. But SOA might be more interested in collecting additional information, some of which would contribute valuable intelligence, devoid of any value to the justice system. And it is possible for neither side to benefit, or even worse, that one or both suffer damaging setbacks: for instance, losing a case; a failed operation; losing a valuable asset; or a damaged reputation. None of these scenarios can be predetermined.

A practical and probably most frequent form of cooperation is when SOA has information that might be useful to criminal investigators or authorities. It is usually in the form of 'lead information' which may or may not be acted upon, as it is up to law enforcement to decide. SOA is bound by law to report information it collects that indicate criminal activity to prosecutors (DORH).[344] But it is not obliged to share other information which could be useful to the police, the prosecutor's office, or any other relevant state bodies. Unfortunately, due to the classified nature of SOA's work, no public data is available that would indicate how often information is given and how useful it is to law enforcement bodies. But SOA's growing transparency seems to suggest it happens quite frequently.[345]

344 NN (Narodne Novine/Official Gazette), 2006. *Zakon*, Article 56.

345 SOA – Security Intelligence Agency, 2023. *Public Report 2022.* Zagreb: SOA. Available at: https://www.soa.hr/files/file/Javno-izvjesce-2017.pdf [Accessed 10 May 2025], 23-24.

SOA's support to law enforcement bodies has been openly confirmed in its annual public reports, although it rarely if ever mentions or confirms its role in specific cases. The circumstances its public reports mention include instances of corruption, money laundering, terrorist financing, organized crime, undermining public procurement, illicit trafficking, and illegal migration. SOA has also been known to alert civil authorities over high-risk events, including sporting matches (fan violence), concerts, and other large public gatherings. Violent western Balkans gangs and crime groups, regional networks of illicit trafficking, and radicalized Balkan fighters returning from Syria, represent complex dilemmas. Civil authorities and the police have come to greatly rely on the intelligence support from SOA. Intelligence assessments on irregular migration, a rampantly dynamic phenomenon across the region, are highly valued by Croatia's border police and other relevant institutions. War crimes and searching for missing victims from the war has also featured on SOA's agenda. On rare occasions, the Agency is publicly acknowledged. 'The police are investigating this case in close partnership with SOA,' stated deputy Prime Minister and Minister of the Interior Davor Božinović at a press conference after a nation-wide wave of false bomb threats caused public uneasiness.[346]

The information it provides to other authorities, as far as SOA is concerned, does not necessarily have to produce criminal convictions. The police and prosecutors are often judged on the merits of cases that end in successful prosecutions. For the police, it is about the evidence they collect and the arrests they make. For the prosecutor, it is about a well-prepared evidence-based argument in court hearings. And in high-profile cases, both are exposed to media and public scrutiny. SOA is fundamentally different, and unless it is pushed to do so, it would rather stay out of the limelight. It could just as well achieve its mission simply through prevention. It wants to collect and distribute 'actionable information'. For example, say SOA obtained information of a (criminal) conspiracy to undermine an important government contract or a large public tender. If, after receiving the information from SOA, the proper authorities terminated the process and prevented any damage, SOA would have served its purpose. This is despite the fact that none of the conspirators would be brought to justice.

There are limits to SOA's support to law enforcement bodies. Intelligence information cannot be used as evidence in criminal proceedings and restrictions may exist in other non-criminal cases. This is understandable because of the fundamental difference in the due process standards of criminal investigations and those of intelligence collection, as well as strict statutory procedures on protecting classified information. An exception exists, according to Article 187 of Croatia's Criminal Procedure Law, when intelligence information helps verify a perpetrator's identity in an assassination of high government official and in cases of terrorism; this includes financial and other support to terrorists. There are other more controversial possibilities. In a case involving a serious crime, according to Article 10 of the above-mentioned law, a presiding judge has discretionary powers

346 Government of Croatia, 2022. 'Božinović'.

to decide on the use of evidence that has not been legally obtained. In doing so, the judge would have to decide that the interests of the criminal prosecution prevail over a defendant's rights. However, the use of (declassified) intelligence information under Article 187 would be highly contentious and has never been tested in a Croatian court.

Intelligence information is not necessarily always inadmissible in court proceedings, but it is limited by levels of classification (top secret, secret, confidential, or restricted). There are also strict procedural norms that protect a party's right to a fair trial. SOA, as the proprietor, can decide to declassify information it produces, making it potentially more readily available to be used in court. If the information comes from one of SOA's many international partners, the third-party rule usually applies, requiring the original owner's approval before it can be shared or used in any other way (declassified). Problems usually arise when classified information cannot be made publicly available due to national security concerns. A judge may have access to intelligence information and can use that information in making a ruling. However, laws protecting classified information prevent the judge from using classified content in judicial rulings, which are public documents. Cases involving petitions for citizenship, requests for extended stay, work permits, and visa entries, where authorities have rejected requests based on intelligence have particularly hampered procedures. For a good account of the use of intelligence information in criminal and non-criminal court procedures in Croatia see DCAF.[347]

SOA's initiatives in developing open-source intelligence and cybersecurity capabilities also have a high value potential in law enforcement. In 2023, SOA established an international open-source intelligence centre of excellence (OSINT) in Zagreb. 'Intelligence is no longer only about secrets, write Levesque and Walton, it's increasingly 'about using data to see clearly, decide quickly, and move first'.[348] A dozen international partners have signed on, with many already actively participating. The centre is envisioned as a hub for improving skills and expertise. The centre will include in its remit technological advancements (including artificial intelligence) and the social media transformation of the exponentially growing availability of vast amounts of public data, information, and knowledge. As such the centre will surely be an asset to law enforcement bodies in Croatia and for its partners.

SOA and Croatia's law enforcement bodies have worked closely together on cybersecurity, an emerging challenge equally concerning to both. In 2024, the National Cyber Security Centre was established within SOA. Consistent with the requirements of the EU's NIS2 Directive, the Centre is an offshoot of SOA's decade-old commitment to creating cyber capacities. It was already running a national umbrella-like sensor network (SK@UT) and was one of the lead agencies in dealing with cybersecurity incidents. While these cyber responsibilities further

347 DCAF, 2021. 'Admissibility of (Counter-) Intelligence Information as Evidence in Court'. Research Paper. Geneva: DCAF, 14-16.

348 Levesque, G and Walton, C., 2025. 'The Future of Intelligence is Open'. *Foreign Policy*. 8 October.

add to SOA's many other tasks, it is likely to morph into a national enterprise entirely separate from the Agency. As such, the Centre would still be expected to continue supporting both public order (policing) and national security missions.

Inquiries of individual complaints or news reports of wrongdoing in the intelligence community have been relatively effective as of late. While public trust in SOA has not been measured, recent media reports would suggest a growing trend in public confidence. Equally important, the administrative (UVNS), parliamentary and civilian oversight bodies are now well-established and able to exercise independent supervision. Each has a unique and complementary role in assuring SOA lawfully and effectively accomplishes its mission. Few Western democracies can measure up to Croatia's three-tier oversight coverage and the full potential of its oversight mandate.[349] The oversight mechanism is also best placed to ensure accountability. One of the most publicized inquiries into misappropriation of public funds resulted in the arrest of leading officials in SOA's military sister service. With confidence in the work of oversight bodies, Croatia's Ombudsman and a parliamentary committee on human rights protection have hardly been called upon to act. Contrast this with the case twenty years ago when a young journalist's rights were abused by the domestic security service. Since then, Croatia has also adopted whistleblower protection legislation, an EU-wide common standard. An exemption allows security and defence bodies to develop their own internal regulations that provide employees with the ability to report irregularities and wrongdoing without having to face retaliatory consequences.

3.2.5. Conclusion

It would be difficult to conclude that Croatia's decision to separate law enforcement and intelligence powers, now well over twenty years ago, had resulted in 'symbiotic mutualism' (where both benefit). But, at the very least, it has quelled risks of a single service wielding broader intelligence-police powers indiscriminately—increasing the potential of undermining due process, infringing on rights and freedoms, or falsely using a national security pretext. At most, each side of the security ledger should be better off at doing what it does best, be it fighting crime or collecting and analysing information. Croatia's law enforcement and intelligence bodies have been able to develop their own set of skills and capacities. They have not always seen eye to eye and, more often than not, they have disagreed on the best course of action when their competing interest in a particular case overlapped. But Croatia's law enforcement and intelligence bodies have each developed their own distinct organizational cultures. They would probably want to keep it that way. Speaking to senior police and intelligence officials, I am hard pressed to find anyone who believes otherwise. Both have also found a way to coexist in a world of increasingly complex challenges, challenges which continually test the limits of how well they are able to cooperate and work together.

349 See NN (Narodne Novine/Official Gazette), 2006. Zakon, Articles 103-114.

3.3. Finnish case study: Intelligence oversight

Mikael Lohse

3.3.1. Intelligence legislation

Civilian and Military Intelligence laws[350] entered into force in Finland on 1 June 2019. This was some 107 years after the emergence of independent Finnish Military Intelligence[351] and 76 years after the establishment of the Finnish Security Police, nowadays known as the Finnish Security and Intelligence Service[352] (FSIS). After the Cold War, the foreign policy reasons for restricting intelligence came to an end. In the early 1990s, Finland unilaterally withdrew from the military provisions of the Paris Peace Treaty and the Finno-Soviet Agreement of Friendship, Cooperation, and Mutual Assistance ceased to be in force. Since then, the restrictions on intelligence have been self-imposed.[353] With the FSIS and Finnish military intelligence authority securing new statutory powers to collect and use information about both domestic and foreign threats to Finland's national defence and security, these authorities have been transformed into combined domestic security and foreign intelligence services. The intelligence reform represents the most profound change ever made in the Finnish security sector.[354]

The intelligence law reform included not only legislation on civilian and military intelligence, but also the Act on the Oversight of Intelligence,[355] the amendment of Parliament's Rules of Procedure,[356] as well as the amendment of section 10 of the Constitution of Finland on the right to privacy.[357] According to the new section

350 Civilian intelligence legislation consists of two legal instruments: the amendment (Chapter 5a) to the Police Act 581/2019 and the Act on Civilian Intelligence Gathering on Network Traffic 582/2019. The provisions on military intelligence can be found in the Act on Military Intelligence 590/2019.

351 Finnish Defence Forces, 2025. *Military Intelligence Review 2025*, 7. Available at: https://puolustusvoimat.fi/documents/1948673/2014902/PV_sotilastiedustelu_raportti_EN_2025_web.pdf/c0125ed9-1467-23e7-e7b6-a7891c4fb5fe/PV_sotilastiedustelu_raportti_EN_2025_web.pdf?t=1737033107374./ [Accessed 4 November 2025]

352 Finnish Security and Intelligence Service, 2023. *Yearbook 2023*, 10. Available at: https://supo.fi/documents/38197657/40760242/SUPO%20Yearbook%202023.pdf/1cbc146a-5d16-ccbb-e146-09a189d76dab/SUPO%20Yearbook%202023.pdf?t=1711371589730. [Accessed 4 November 2025]

353 Lohse, M. and Viitanen, M., 2019. *Johdatus tiedusteluun* [Introduction to intelligence]. Alma Talent, 17.

354 Lohse, M., 2020. 'The Intelligence Process in Finland'. *Scandinavian Journal of Military Studies,* 68. Available at: https://sjms.nu/articles/10.31374/sjms.55, [Accessed 4 November 2025]

355 Intelligence Oversight Act 121/2019, 2019.

356 The Parliament's Rule of Procedure 40/2000, 2000. [online]. Available at: https://www.finlex.fi/sv/lagstiftning/2000/40. [Accessed 4 November 2025]

357 The Constitution of Finland 731/1999, 1999. [online] Available at: https://www.finlex.fi/en/legislation/translations/1999/eng/731. [Accessed 5 November 2025]

10 (4) of the Constitution of Finland 'Limitations of the secrecy of communications may be imposed by an Act if they are necessary […] for the purpose of obtaining information on military activities or other such activities that pose a serious threat to national security'. The constitutional amendment was a prerequisite for the introduction of intelligence laws. It entered into force on 15 October 2018[358] whereas the Act on the Oversight of Intelligence and amendment of Parliament's Rules of Procedure entered into force on 1 February 2019.[359]

3.3.2. Civilian and military intelligence

The Finnish Security and Intelligence Service is responsible for civilian intelligence and the military intelligence authorities for military intelligence. They are empowered to discharge their functions using a range of 24 statutory information gathering methods, together with certain customary legal approaches.[360]

Section 1 of Chapter 5a of the Police Act defines civilian intelligence as the gathering of information by the FSIS and the use of information to safeguard national security, to substantiate top-level government decisions, and for the statutory tasks of other authorities in the field of national security. In practice, FSIS produces intelligence information to provide early warning of potential measures against Finland, and especially Russia's non-military hostile activities towards Finland.[361] In addition, FSIS counters terrorism and espionage, and grants security clearances.[362]

The purpose of military intelligence is to acquire and process information on military activities that target Finland or that endanger functions vital to Finnish society.[363] That information is needed, so that military intelligence can give the necessary early warning of any military threat against Finland. It is also necessary for creating the necessary situational awareness to support the decision-making of the Defence Forces and the state leadership, and to create the necessary situational awareness to support the execution of the statutory tasks of the Defence Forces.

358 Finnish Government, 2018. *Press release*. Available at: https://valtioneuvosto.fi/-/1410853/luottamuksellisen-viestin-suojaa-koskeva-perustuslain-muutos-voimaan-lokakuussa?languageId=en_US. [Accessed 5 November 2025]

359 Finnish Government, 2019. *Press release*. Available at: https://valtioneuvosto.fi/-/1410853/tiedustelutoiminnan-valvontaa-koskeva-laki-voimaan-helmikuun-alusta. [Accessed 5 November 2025]

360 Lohse, M., Meriniemi, M. and Honkanen, K., 2022. *Tiedustelumenetelmät* [Intelligence Gathering Methods]. Alma Talent, 17–18.

361 Finnish Security and Intelligence Service, 2025. *National Security Overview 2025*, Director's foreword. Available at: https://katsaus.supo.fi/en/director-s-foreword. [Accessed 5 November 2025]

362 Finnish Security and Intelligence Service, *Yearbook 2023*, 15.

363 Section 3 of the Act on Military Intelligence.

These tasks consist in the military defence of Finland, providing support for other authorities, providing and receiving international support, and participating in international military crisis management.[364]

The duties of the FSIS and the military intelligence authorities also include the prevention and detection of offences threatening national defence and security. However, FSIS is not a pre-trial investigation authority and does not, therefore, investigate criminal offences.[365] The same applies to military intelligence authorities. According to Section 86 of Chapter 9 of the Act on Military Discipline and Combating Crime in the Defence Forces (255/2014), the National Bureau of Investigation is responsible for investigating any offence related to intelligence activities directed at Finland in terms of military national defence, as well as any other offences that threaten the objectives of that defence.

FSIS is an agency of the Ministry of the Interior that operates in Finland and abroad. From a legal point of view, FSIS remains a national police unit.[366] FSIS headquarters is located in Helsinki, but the organisation operates throughout national territory. The service has eight regional departments that are responsible, together with operational departments, for FSIS functions outside the Helsinki Metropolitan Area.[367]

Military intelligence, including counterintelligence, is a part of the operational activities of the Defence Forces. The Ministry of Defence is responsible for the administrative guidance of military intelligence.[368] The military intelligence authorities are the Defence Command and the Finnish Defence Intelligence Agency.[369] The planning and execution of military intelligence tasks is led by the Defence Command Chief of Intelligence, who also steers the Finnish Defence Intelligence Agency.[370]

364 Section 2 (1304/2022) of the Act on the Defence Forces.

365 Section 1 of Chapter 2 of the Criminal Investigation Act 805/2011.

366 Section 1 (860/2015) of the Act on Police Administration.

367 Finnish Security and Intelligence Service. The organisation of FSIS. Available at: https://supo.fi/en/organisation1. [Accessed 5 November 2025]

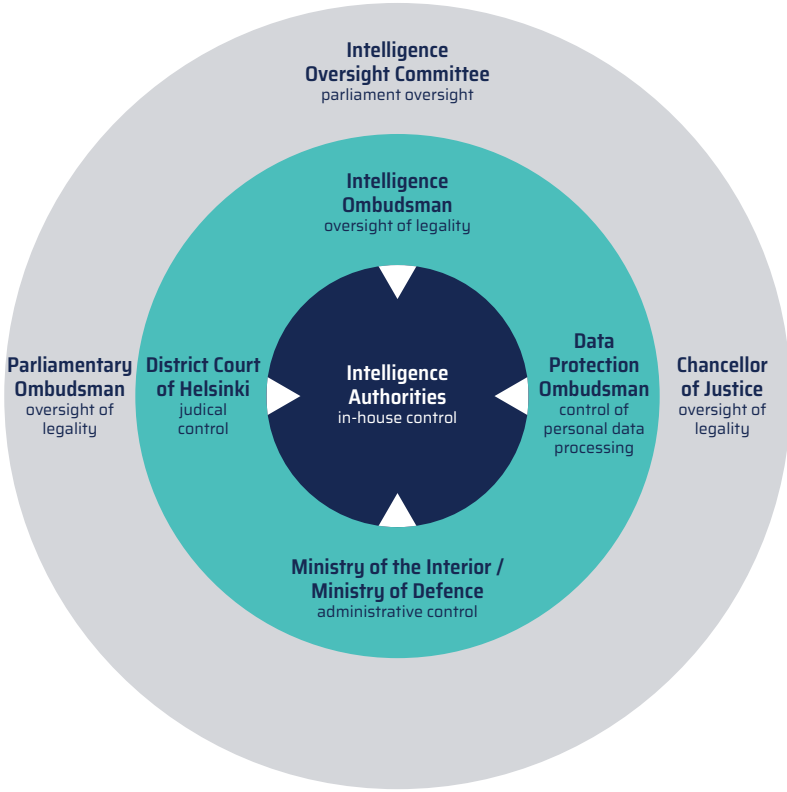
368 Section 13 of the Act on Military Intelligence.

369 Section 11 of the Act on Military Intelligence.

370 Finnish Defence Forces, *Military Intelligence Review 2025*, 28–31.

3.3.3. Formal oversight system

In Finland, several actors participate in the oversight of intelligence activities. This model, based on cooperation between the internal and external overseers of intelligence activities, enables supervision from multiple angles and the cost-effective use of special expertise. The figure below illustrates the organisation of intelligence oversight and court control in Finland.



3.3.3.1. Internal oversight

In addition to regular managerial steering, the internal supervision of intelligence activities includes the intelligence authorities' internal legality supervision.[371] In the Finnish Security and Intelligence Service, this is the remit of the Service's internal overseer of legality. In the military intelligence authorities, in-house control is executed by the Defence Command Legal Division under the Chief Legal Advisor

371 Finnish Security and Intelligence Service. Intelligence operations are strictly supervised in Finland. Finnish Security Intelligence Service, n.d. *Regulatory Control*. Available at: https://supo.fi/en/regulatory-control. [Accessed 4 November 2025]

of the Defence Forces.[372] The legality oversight is conducted by quarterly and thematic inspections.[373] Notifications to the Intelligence Ombudsman are essential. The intelligence authorities are to give information to the Intelligence Ombudsman on authorisations and decisions concerning intelligence collection methods, issued as soon as the authorisation is granted, or the decision made.[374]

Administrative control of FSIS by the Ministry of the Interior[375] and that of the military intelligence authorities by the Ministry of Defence is also included in internal supervision. Among other things, the Ministry of the Interior and Ministry of Defence are tasked with ensuring that Finnish intelligence authorities appropriately organise their operations, issue guidelines, train their personnel and arrange their internal supervision of legality. These tasks are safeguarded by reporting obligations and access rights. The Head of FSIS must, without prejudice to the provisions on secrecy, inform the Minister of the Interior, the Permanent Secretary of the Ministry of the Interior, and the Head of the National Security Unit of matters of social importance.[376] The Ministry of Defence has, notwithstanding secrecy provisions, the right to obtain information on issues related to military intelligence which are of social or economic importance or of serious significance.[377]

3.3.3.2. External oversight

The external supervision of intelligence activities is mainly conducted by the Intelligence Ombudsman and the Intelligence Oversight Committee of Parliament. The Intelligence Ombudsman is responsible for legality oversight of intelligence activities while parliamentary oversight is run by the Intelligence Oversight Committee. The Data Protection Ombudsman also has a role to play, albeit a rather narrow one.

Legal oversight by the Intelligence Ombudsman

The Intelligence Ombudsman is tasked with supervising the legality of intelligence gathering methods and the use of intelligence, as well as the legality of other intelligence operations conducted by FSIS and the military intelligence authorities. The Intelligence Ombudsman operates independently.[378]

372 Section 105 of the Act on Military Intelligence.

373 Finnish Defence Forces, *Military Intelligence Review 2025*, 34-36.

374 Section 61 of Chapter 5a of the Police Act, Section 26 of the Act on Civilian Intelligence Gathering on Network Traffic, and Section 108 of the Act on Military Intelligence.

375 Section 59 of Chapter 5a of the Police Act.

376 Section 4a (556/2020) of the Act on Police Administration.

377 Section 106 of the Act on Military Intelligence.

378 Section 2 and 5 of the Act on the Oversight of Intelligence.

The Intelligence Ombudsman is also tasked with:

- supervising the respect of fundamental and human rights in intelligence activities;
- promoting legal protection and adherence to related best practices in intelligence activities; and
- monitoring and assessing the functionality of legislation in the Ombudsman's purview and proposing improvements when necessary.[379]

The Intelligence Ombudsman obtains the information and reports required for the performance of its oversight duties from authorities and other bodies with public administration duties. The Ombudsman may also conduct announced or unannounced inspections on the premises of authorities and other bodies with public administration duties. These visits are to supervise the legality of intelligence activities. In connection with such inspections, the Ombudsman has the right to access the premises and information systems necessary for the supervision of the authority or body.[380]

The Intelligence Ombudsman has the right to attend and speak at sessions of the Helsinki District Court concerning the authorisation of intelligence gathering methods. The Intelligence Ombudsman may complain to the Court of Appeal about decisions of the District Court, but the supervision of the legality of the court's activities does not fall under the duties and powers of the Ombudsman.[381]

The Intelligence Ombudsman seeks to ensure the legality of intelligence activities primarily by informing the subject of the supervision of the Ombudsman's opinion of legal procedure, good governance and the promotion of fundamental and human rights. If the Ombudsman finds that the subject of supervision has violated the law in its intelligence activities, the Ombudsman can ultimately order the intelligence gathering method to be suspended or terminated. The Ombudsman may also refer the matter to the pre-trial investigation authority.[382]

The Intelligence Ombudsman performs *ex ante* (advance), *ex durante* (real-time) and *ex post* (retrospective) supervision of the legality of the use of intelligence gathering methods.[383] Part of advance oversight is participation in the training and other competence development of public officials charged with the application of the intelligence legislation.

379 Section 7 of the Act on the Oversight of Intelligence.

380 Section 8, 9, and 10 of the Act on the Oversight of Intelligence.

381 Section 14 of the Act on the Oversight of Intelligence.

382 Section 15, 16, 17, and 18 of the Act on the Oversight of Intelligence.

383 Lohse, M. and Viitanen, M., 2019. *Johdatus tiedusteluun,* 141.

The Office of the Intelligence Ombudsman checks the decisions of the intelligence authorities on the use of intelligence gathering methods and intelligence management. This real-time oversight of legality is supported by the intelligence authorities' obligation to inform the Intelligence Ombudsman of decisions on intelligence gathering methods without delay, and, in any case, prior to implementation.[384] The Office of the Intelligence Ombudsman also sends participants to the Helsinki District Court's sessions on intelligence gathering methods. In fact, the Ombudsman is represented in all such court sessions.[385]

Inspecting the records drawn up on the use of intelligence gathering methods is part of the Intelligence Ombudsman's retrospective oversight of the legality of intelligence activities. One theme of retrospective oversight is the supervision of the checking, storage, archiving and further use of material obtained through intelligence gathering.[386]

Anyone who considers that their rights have been infringed in the course of intelligence activities or that such operations have otherwise broken the law can file a complaint to the Intelligence Ombudsman; so long, of course, as the issues fall under the Ombudsman's remit. A person subjected to intelligence gathering or who suspects that they have been subject to intelligence gathering can ask the Intelligence Ombudsman to investigate the lawfulness of the use of such methods.[387] The number of investigation requests and complaints made to the Intelligence Ombudsman have varied between seven and twenty annually.

The Intelligence Ombudsman must share significant findings with the Intelligence Oversight Committee of Parliament. The Ombudsman also submits an annual report on his or her activities to Parliament, the Parliamentary Ombudsman, and the Government.[388]

384 Section 61 of Chapter 5a of the Police Act, section 26 of the Act on the Use of Network Traffic Intelligence in Civilian Intelligence, and section 108 of the Act on Military Intelligence.

385 Intelligence Ombudsman, 2023. *Annual Report 2023*, 11. Available at: https://tiedusteluvalvonta.fi/documents/12994206/0/1%20TVV%20vuosikertomus%20www%202023.pdf/4295ddcc-7a3a-6b84-d9d1-78ac0c2a3ba4/1%20TVV%20vuosikertomus%20www%202023.pdf. [Accessed 5 November 2025]

386 Intelligence Ombudsman, n.d. *Forms of oversight*. Available at: https://tiedusteluvalvonta.fi/en/forms-of-oversight. [Accessed 5 November 2025]

387 Section 11 and 12 of the Act on the Oversight of Intelligence. See also Act on the Oversight of Intelligence, n.d. *Complaints and Investigation Requests*. Available at: https://tiedusteluvalvonta.fi/en/complaints-and-investigation-requests. [Accessed 5 November 2025]

388 Section 18 and 19 of the Act on the Oversight of Intelligence. See also Intelligence Ombudsman (TVV), 2023. *Annual Report 2023*. Available at: https://tiedusteluvalvonta.fi/documents/12994206/0/TVV%20Annual%20report%202023%20summary%20A.pdf/f5446c9e-4dda-be13-f9ab-8a1ac4b96ff3/TVV%20Annual%20report%202023%20summary%20A.pdf. [Accessed 5 November 2025]

Parliamentary oversight by the Intelligence Oversight Committee

The Intelligence Oversight Committee serves as the parliamentary watchdog of civilian and military intelligence operations. The committee also serves as the parliamentary watchdog of the other activities of FSIS.[389] The Intelligence Oversight Committee is established after the Government has been appointed following the parliamentary elections, unless Parliament decides otherwise based on the Speaker's Council's proposal.[390] The Intelligence Oversight Committee has eleven permanent members and two deputy members.

As part of its parliamentary oversight role, the Intelligence Oversight Committee oversees the proper implementation and the appropriateness of intelligence operations. It monitors and evaluates the direction of intelligence operations, monitors and promotes the effective exercise of fundamental and human rights in intelligence operations, prepares reports based of the work of the Intelligence Ombudsman and processes the supervisory findings of the Intelligence Ombudsman.[391] The Intelligence Oversight Committee may, on its own initiative, bring up any matter within its authority for processing. It may hold closed meetings. It may also prepare a report for a plenary session if it regards a given matter to be significant enough.

The Intelligence Oversight Committee have extensive access rights to all intelligence-related information. These rights of access do not depend on the secrecy of the information or documents. Rather they extend to all levels of classification. It is also within the exclusive competence of the committee to assess what information is necessary for the purpose at hand.[392] In return for strong access rights, the members of the Intelligence Oversight Committee are subject to extensive security clearance vetting.[393] The committee members are also bound by secrecy and confidentiality: classified documents may not be disclosed or divulged to third parties and confidentiality here also covers non-recorded information, such as conversations intended to be private.[394]

389 Parliament of Finland, n.d. Intelligence Oversight Committee. Available at: https://www.eduskunta.fi/EN/valiokunnat/tiedusteluvalvontavaliokunta/Pages/default.aspx. [Accessed 5 November 2025]

390 Section 17 of the Parliament's Rules of Procedure.

391 Section 31b of the Parliament's Rules of Procedure.

392 Lohse, M., 2023. 'Finnish intelligence overseers' right of access supersedes Originator Control'. *about:intel*. Available at: https://aboutintel.eu/finnish-intelligence-overseers-right-of-access-supersedes-originator-control/. [Accessed 5 November 2025]

393 Section 17a of the Parliament's Rules of Procedure.

394 Section 43b and 43c of the Parliament's Rules of Procedure.

Control of personal data processing by the Data Protection Ombudsman

The Act on the Oversight of Intelligence has not changed the tasks and powers of the Data Protection Ombudsman. The Ombudsman's tasks include, among other things, the promotion of public awareness on the risks, legislation, safeguards, and rights related to the processing of personal data and the provision of information to data subjects, upon request, on the exercise of their rights.[395] The powers of the Data Protection Ombudsman are wide-ranging. They cover, for example, the right to order the data controller – such as FSIS and the military intelligence authority – to notify the data subject of a personal data breach. He or she can impose a temporary or permanent ban or other restrictions on processing. They can order the suspension of data transfer to a recipient in a third country or to an international organisation.[396]

The Data Protection Ombudsman has the right to receive, without prejudice to the provisions on secrecy, any information necessary for the performance of his or her duties from being a data controller to carrying out an inspection at the premises of the controller.[397] The Data Protection Ombudsman will without delay draw up a written report on any inspection, indicating the progress of the inspection and the main findings made by the Ombudsman. The inspection report is communicated to any party entitled to be present during the inspection.[398]

In principle, everyone has the right to be informed by the controller whether personal data concerning them are being processed. However, the data subject's right of access may be restricted if this is proportionate and necessary for the protection of national security. If (and when) the data subject's right of access is denied, he or she can request the Data Protection Ombudsman to verify the lawfulness of the personal data being collected and their processing. Where the data subject exercises such indirect right of access, the Data Protection Ombudsman is to, within a reasonable time, inform the data subject of the measures taken.[399] In practice, the Ombudsman checks on the lawfulness of the processing of personal data of several requested persons during a single visit to the intelligence authority.[400]

395 Section 46 of the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018).

396 Section 51 of the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security.

397 Section 47 and 48 of the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security.

398 Lohse, M. and Viitanen, M., 2019. *Johdatus tiedusteluun*, 155.

399 Section 23, 24, 28 and 29 of the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security.

400 Lohse, M. and Viitanen, M., 2019. *Johdatus tiedusteluun*, 156.

Oversight of legality by the supreme guardians of the law

The system of external supervision is complemented by the supreme guardians of law, that is, the Parliamentary Ombudsman and the Chancellor of Justice. They both have the right to receive from public authorities or other performing public duties information needed for their supervision of legality.[401] According to the division of duties between the supreme guardians of law, the Parliamentary Ombudsman supervises the operative dimension of intelligence activities, and the Chancellor of Justice supervises the same at the strategic level.

The Ministry of the Interior issues an annual report on the use of intelligence gathering methods and measures to protect civilian intelligence, as well as on the oversight to the Parliamentary Ombudsman.[402] The Ministry of Defence has the same obligation to inform the Ombudsman about the state of military intelligence and its oversight.[403] So, as the supreme guardian of the law, the Parliamentary Ombudsman also exercises control over oversight. This includes: control over the Intelligence Ombudsman and Data Protection Ombudsman.[404] The Parliamentary Ombudsman submits an annual report to the Parliament on his or her work, including observations on the state of the administration of justice and on any shortcomings in legislation.

Ex ante authorization by Helsinki District Court

Even though the independent courts are not supervisory authorities, they play an essential role in the intelligence control system by ensuring legal protection. The intelligence authority cannot have unlimited discretion in deciding on the use of an intelligence gathering method. Deployment of the intelligence gathering methods which represent the deepest infringement on the fundamental and human rights of an individual are authorised by district judges in the Helsinki District Court.[405] There are twelve such methods out of a total of 24 statutory intelligence gathering methods. The judge decides, among other things, on the use of telecommunications interception and network traffic intelligence. Organisational centralisation has been introduced to ensure that the court has strong knowledge and expertise in matters concerning the use of an intelligence gathering method.[406]

401 Section 111 of the Constitution of Finland.

402 Section 60 of Chapter 5a of the Police Act.

403 Section 107 of the Act on Military Intelligence.

404 Parliament Ombudsman in Finland, 2023. *Special theme in 2023: Oversight of oversight*, 121. Available at: https://www.oikeusasiamies.fi/documents/20184/39006/summary2023_web.pdf/b345ccec-4284-785f-3472-5f9a7e45e152?t=1727946629802. [Accessed 4 November 2025]

405 Lohse, M., 2020. 'The Intelligence Process', 73.

406 Lohse, M. and Viitanen, M., 2019. *Johdatus tiedusteluun*, 149.

The district court has a quorum with only the chairperson present. The composition shall be, and usually is, supplemented with a legally trained member.[407]

A request to use an intelligence gathering method is to be made in writing. The Intelligence Ombudsman is notified of a request concerning an intelligence collection method submitted to a court.[408] The intelligence authority has the obligation to provide the court with this information, and the burden of proof, that the general and specific conditions for the use of the intelligence gathering method are fulfilled, rests with the authority. A request to use an intelligence collection method is to be considered by a court without delay in the presence of the intelligence officer who made the request. The court shall give the Intelligence Ombudsman, or a public official designated by the Ombudsman an opportunity to be heard in the hearing. The matter shall be decided urgently, and the decision must be given immediately.

No judicial review may be requested by way of appeal in respect of decisions issued in matters concerning authorisations. A complaint may be filed against the decision to the Helsinki Court of Appeal: there is no time limit on this. The Intelligence Ombudsman also has the right to file a complaint against a decision given in a matter concerning the granting of an authorisation for the use of a given intelligence collection method.[409]

3.3.4. Informal accountability mechanisms

One of the most visible non-governmental organisations in the field of intelligence oversight is Electronic Frontier Finland (Effi). Effi tries to influence legislative proposals concerning, for example, personal privacy by statements, press releases, and engaging in public policy and legal discussion. Effi is a founding member of European Digital Rights (EDRi).[410] According to Effi's statement, it is difficult to assess the functioning of intelligence oversight without public information on which to base an assessment.[411]

According to Joonas Widlund, one of the most prominent debaters on intelligence oversight in Finland, the requirement for pro-activity and cooperation in the

407 Section 11 (422/2018) of Chapter 2 of the Code of Judicial Procedure.

408 Section 61 of Chapter 5a of the Police Act, Section 26 of the Act on Civilian Intelligence Gathering on Network Traffic, and Section 108 of the Act on Military Intelligence.

409 Section 35 of Chapter 5a of the Police Act, Section 8 of the Act on Civilian Intelligence Gathering on Network Traffic, and Section 116 of the Act on Military Intelligence.

410 Electronic Frontier Finland. Available at: https://effi.org/in-english/. [Accessed 4 November 2025]

411 **EFFI**, 2022. *Statement to the Transport and Communications Committee of the Parliament, 10 March 2022.* [online] Available at: https://effi.org/wp-content/uploads/2022/03/2022-03-10_Effi_lausunto_lvv_-tiedustelulaki.pdf. [Accessed 5 November 2025]

supervisory network is strong. Extensive access rights enable effective oversight, but the oversight body must also be willing and able to make use of this opportunity: this means cooperation between the overseers. Widlund notes that the Intelligence Ombudsman's annual report does not contain very detailed comments on intelligence activities.[412]

Widlund also says that there are certain aspects where the IOC (Intelligence Oversight Committee) appears weaker than its international counterparts. In his view, the reason for this lies in the division of duties between the IOC and the Intelligence Ombudsman. It must be acknowledged that this kind of division in terms of the oversight bodies involved and the nature of their duties appears characteristic to the Finnish system. This arrangement of close cooperation and support between two external oversight bodies, one parliamentary and the other independent (though parliament-adjacent), allows the IOC to focus more on tasks it is better equipped to handle, such as intelligence priorities and resourcing needs.[413] As long as cooperation between the two external oversight bodies remains functional, the IOC should not be in danger of becoming a blind guardian, since the Ombudsman plays a major role in providing the IOC information through reports.[414]

Themes related to intelligence receive quite frequent media attention. The biggest scandal has been caused by an article in the Helsingin Sanomat newspaper entitled 'A secret under a rock – hardly anyone knows what the Defence Forces' Communications Centre does, but now documents obtained by Helsingin Sanomat unlock the mystery.'[415] As a result, the Court of Appeal of Helsinki found two journalists guilty of the disclosure of a national secret and of an attempt to such offence. One of the journalists was sentenced to four months' conditional imprisonment and the other to a sentence of 80 days fine.[416] Another news story with significant consequences was published under the title 'Finland's intelligence activities are the subject of an extraordinary criminal allegation – Here's what we know about the case'.[417] The Deputy Prosecutor General ordered a preliminary

412 Widlund, J., 2021. 'Tieto, valta ja tiedustelun valvonta: Tiedusteluvalvontavaltuutetun arviointia [Information, power and intelligence oversight: An evaluation of the Intelligence Ombudsman]'. *Oikeus*, 204–205. Available at: https://osuva.uwasa.fi/bitstream/handle/10024/18227/978-952-395-168-6.pdf?sequence=2&isAllowed=y. [Accessed 4 November 2025]

413 Lohse, M., 2023. 'Finnish intelligence overseers' right'.

414 Widlund, J., 2023. 'More Than Just Blind Guardians?'. *Scandinavian Studies in Law,* 93. Available at: https://scandinavianlaw.se/pdf/69-4.pdf. [Accessed 4 November 2025]

415 Helsingin Sanomat, 2017. *'A secret under a rock – hardly anyone knows what the Defence Forces' Communications Centre does, but now documents obtained by Helsingin Sanomat unlock the mystery'*, 16 December 2017. Available at: https://www.hs.fi/politiikka/art-2000005492284.html. [Accessed 5 November 2025]

416 The Court of Appeal of Helsinki, 2025. *Press release, 1 July 2025.* Available at: https://tuomioistuimet.fi/hovioikeudet/helsinginhovioikeus/fi/index/tiedotteet/2025/kahdenhelsinginsanomientoimittajankatsottiinsyyllistyneenturvallisuussalaisuudenpaljastamiseenjaturvallisuusalaisuudenpaljastamisenyritykseenniinsanotussaviestikoekeskus-asiassa.html. [Accessed 5 November 2025]

417 Helsingin Sanomat, 2024. *'Finland's intelligence activities are the subject of an extraordinary criminal allegation – Here's what we know about the case'*, 8 May 2024. Available at: https://www.hs.fi/suomi/art-2000010411966.html. [Accessed 4 November 2025]

investigation in this case reported to the Prosecution Authority by the Intelligence Ombudsman.[418] Due to this suspicion, the Parliamentary Office Commission decided to suspend the Secretary General Antti Pelttari from his office for the duration of the preliminary investigation. Before becoming Secretary General, Pelttari had served as head of FSIS.[419] Military intelligence has not escaped scandal either. A former head of Finnish Military Intelligence and the EU Military Staff Georgij Alafuzoff was sentenced to one year and ten months in prison for aggravated service offence. Alafuzoff had unlawfully stored confidential and classified military intelligence information at his home.[420]

3.3.5. Evaluation of the oversight system

A crucial precondition for the effective oversight of the Finnish intelligence services' activities is the proper internal control of the services themselves. A clear understanding of the legal obligations of the intelligence services facilitates their effective supervision.[421] Moreover, the findings of intelligence services' in-house control often guide the legality checks of external overseers, too. According to the Intelligence Oversight Committee, both FSIS and the military intelligence authority are professional in the way that they enforce internal control.[422]

The legal framework on external intelligence oversight gives the Intelligence Ombudsman appropriate powers. As a matter of fact, both the Intelligence Ombudsman's and the Intelligence Oversight Committee's access rights are among the most extensive in Europe.[423] Thus, there is no need to amend the legislation. The situation with oversight legislation is the reverse of that with substantive intelligence legislation where several changes are proposed.[424] The government's programme is currently being implemented in the field of

418 Office of the Prosecutor General, 2024. *Press release, 19 December 2024*. Available at: https://syyttajalaitos.fi/-/tutkinnanjohtajan-tiedote-esitutkinta-paatetty-puolustusvoimien-tiedustelutoimintaan-liittyvassa-asiassa. [Accessed 4 November 2025].

419 Helsingin Sanomat, 2025. *'Antti Pelttari is suspended from his position'*, 18 June 2025. Available at: https://www.hs.fi/politiikka/art-2000011307476.html. [Accessed 4 November 2025].

420 The Supreme Court of Finland, 2025. *Press release, 17 June 2025*. Available at: https://korkeinoikeus.fi/fi/index/ajankohtaista/tiedotteet/2025/m412ecx7k.html. [Accessed 4 November 2025].

421 European Union Agency for Fundamental Rights, 2023. Surveillance by intelligence services: Fundamental rights, safeguards and remedies in the EU – 2023 update, 14. Available at: https://fra.europa.eu/en/publication/2023/surveillance-update. [Accessed 5 November 2025].

422 Parliament of Finland, Intelligence Oversight Committee, 2024. Report on the Intelligence Ombudsman's annual report TiVM 2/2024 vp, 16. Available at: https://tiedusteluvalvonta.fi/documents/12994206/0/Valiokunnan%20mietint%C3%B6%20TiVM%202_2024%20vp%20%20K%2014_2024%20vp.pdf/d210a04b-c240-2650-97fb-555b373a4f61/Valiokunnan%20mietint%C3%B6%20TiVM%202_2024%20vp%20%20K%2014_2024%20vp.pdf. [Accessed 5 November 2025]

423 Lohse, 2023. 'Finnish intelligence overseers' right'.

424 Government of Finland, 2023. *Programme of Prime Minister Petteri Orpo's Government*, 203–204. These reforms include, for example, provisions on firewalls between intelligence and criminal justice system, extending intelligence powers to cover premises used for permanent residence, and powers to interfere with a device or software that is located abroad and that is being used for cyber espionage.

intelligence through legislative projects in both the Ministry of the Interior[425] and the Ministry of Defence.[426]

However, broad powers are not themselves a guarantee of effective control. The keys are activity and cooperation, and the quality of reporting. The Intelligence Ombudsman does provide continuous oversight over the use of intelligence collecting methods. According to the Intelligence Oversight Committee, the oversight work by the Intelligence Ombudsman has been good and comprehensive.[427] However, the sharing of information with foreign intelligence services is a common blind spot of oversight systems, not only in Finland, but also in many other Western democracies.[428] It might be worth directing more oversight to intelligence disclosures in international cooperation.

The Finnish model, based on cooperation between the overseers of intelligence activities, enables supervision from multiple angles and the cost-effective use of special expertise.[429] The Intelligence Ombudsman cooperates with the Data Protection Ombudsman in their supervision of the use of intelligence. This is not sufficient. It would be equally useful to coordinate the Intelligence Ombudsman's oversight activities with that of the Ministry of the Interior and the Ministry of Defence.[430] Coordination is needed to avoid duplication of oversight but also to reduce the burden on the auditee.

The intelligence overseers' reports should be in the public domain, and they should contain detailed overviews of the oversight systems and related activities.[431] The annual report of the Intelligence Ombudsman has evolved in these respects for the better. In future, however, the Intelligence Oversight Committee believes that it is appropriate to consider whether it is possible to provide more information on the activities and measures of the Intelligence Ombudsman in the public report itself.[432]

Individuals subject to intelligence do have recourse to remedies that are effective in practice for reviewing the lawfulness and proportionality of any intelligence collection method used against them. They can, also, redress any violations of their rights. The challenge for the Parliamentary Ombudsman is that the

425 Ministry of the Interior. Reform of legislation on civilian intelligence. Available at: https://intermin.fi/en/project/reform-of-legislation-on-civilian-intelligence. [Accessed 4 November 2025].

426 Ministry of Defence. Development of the Act on Military Intelligence. Available at: https://valtioneuvosto.fi/en/projects-and-legislation/project?tunnus=PLM007:00/2024. [Accessed 4 November 2025].

427 Parliament of Finland, Intelligence Oversight Committee, 2024. *TiVM 2/2024 vp*, 7.

428 Widlund, 2023. 'More', 93.

429 Intelligence Ombudsman. Oversight of intelligence. Available at: https://tiedusteluvalvonta.fi/en/oversight-of-intelligence. [Accessed 4 November 2025].

430 Parliament Ombudsman of Finland, 2023. *Annual report 2023*, 180. Available at: https://www.oikeusasiamies.fi/documents/20184/42383/kertomus2023_web2.pdf/be8efe8f-c629-828f-8d03-04a43367eb71?t=1719305126644. [Accessed 4 November 2025].

431 European Union Agency for Fundamental Rights, 2023. Surveillance, 12.

432 Parliament of Finland, Intelligence Oversight Committee, 2024. *TiVM 2/2024 vp*, 16–17.

intelligence activities do not give rise to complaints, which means the main source of Parliamentary Ombudsman information is missing.[433] In 2023, the Intelligence Ombudsman received only eleven investigation requests and one complaint.[434] In all fairness, however, intelligence oversight is not driven by complaints or investigation requests but by the risk-based actions and initiatives of overseers.

Finally, Finland's recent arrival in NATO has implications for the nature and scope of the intelligence overseers' tasks. The Intelligence Oversight Committee urges the government to monitor and assess the adequacy of the resources allocated to intelligence oversight for current and foreseeable future needs.

433 Parliament Ombudsman of Finland, 2023. Annual report 2023, 176.

434 Intelligence Ombudsman, 2023. *Annual Report 2023*, 11. Available at: https://tiedusteluvalvonta.fi/documents/12994206/0/TVV%20Annual%20report%202023%20summary%20A.pdf/f5446c9e-4dda-be13-f9ab-8a1ac4b96ff3/TVV%20Annual%20report%202023%20summary%20A.pdf. [Accessed 4 November 2025].

3.4. French case study: Assessing and overseeing intelligence and law enforcement in the Euro-Atlantic area

Pierre Chambart

3.4.1. French intelligence services with law enforcement mandates

According to the French Government's Vie Publique (Public Life) website[435], 'intelligence is the collection of strategic information on an individual, an institution or a technology and also refers to the administrative cells tasked with collecting the information necessary to identify and prevent any threat (human, material…) that may threaten State security'.

> *The French White Book on Defence from 2008 states that 'intelligence is destined to allow the State's highest authorities, as well as French diplomacy, the Armed Forces, Domestic security and civil security to anticipate and benefit from an autonomy to appreciate, decide and act'.*

For French services to collect intelligence, legal frameworks were put in place in 2015, then in 2017 and they were reinforced in 2021. Promulgated on 24 July 2015 and officially published on 26 July 2015, the law on intelligence,[436] which was the first of its kind in France, aimed at providing a legal framework to the French intelligence services' activities and specifically extended to intelligence purposes the following information-gathering techniques already authorised in a law enforcement judiciary framework,[437] thus making them intelligence techniques:

435 La Rédaction, 2024. 'Renseignement : quelle organisation et quel cadre légal ?' [online] *Vie publique*, 10 September 2024. Available at: https://www.vie-publique.fr/eclairage/272339-renseignement-francais-quel-cadre-legal, [Accessed 28 October 2025].

436 LOI n° 2015-912 du 24 juillet 2015 relative au renseignement, *Journal officiel*, 26 July 2015, n° 0171. Available at: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030931899/ [Accessed 28 October 2025]

437 An investigative judge can authorise investigative units of the National Police and National Gendarmerie to use information-gathering techniques in order to collect technical evidence that will be used in a court of law against suspected criminals. The first highly publicised and effective use of mobile phone locations and phone bills by an investigative unit of the Sous-Direction Anti-Terroriste (SDAT – Sub-Directorate of Anti-Terrorism) of the Direction Générale de la Police Nationale (DGPN – Directorate General of National Police) was made to identify and arrest terrorist suspects linked to the case of the assassination of Prefect Erignac by the so-called Commando Sampieru also named Commando Pasquale Paoli in Ajaccio, Corsica, on 6 February 1998. The use of these techniques was key in identifying the suspected perpetrators and led to their subsequent arrests and confessions.

vehicle marking with beacons; eavesdropping with hidden microphones; filming in private locations; electronic data interception; requesting phone operators to access their networks in case of terrorist threat; control upgrading of detainees' communications; access only to metadata for counterterrorism purposes only; and use of IMSI catchers by specially habilitated personnel.

According to this law, these intelligence techniques could and still can only be used:

- in case of threat to national independence, national defence and the integrity of the national territory.
- for the prevention of terrorism.
- for the prevention of any attack on the republican form of French institutions.
- for the prevention of any attempt to reconstitute dissolved groups.
- for the prevention of collective violent acts susceptible to seriously affect public peace.
- and for the prevention of organised crime.

The law insisted that the most intrusive intelligence techniques could only be employed in accordance with the principle of proportionality and only if there was no available intelligence-gathering method to collect this intelligence.

The law also determined the mandatory administrative procedures for the use of these intelligence techniques. This consists in addressing written motivated requests to the Prime Minister's Office who will then deliver his agreement (or otherwise) after having consulted the Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR – National Committee for the Control of Intelligence Techniques).[438]

The law further stated that its content should be re-examined after a maximum period of five years following a review by the Délégation Parlementaire au Renseignement (DPR – Parliamentary Delegation for Intelligence).[439]

On 30 October 2017, a new law reinforcing domestic security and the fight against terrorism[440] was voted in. It authorised the Minister of Interior to decide on surveillance measures against any individual the behaviour of whom raises serious suspicions that he or she could present a particularly significant threat

438 The CNCTR is an independent administrative authority composed of nine members: two members of the national Assembly; two members of the Senate; two members of the Conseil d'Etat (State Council), which is the highest administrative authority in France; two magistrates of the Court of Cassation, and an expert in electronic communications from the Autorité de Régulation des Communications Electroniques et des Postes (ARCEP – Regulatory Authority of Electronic Communications and Mail).

439 The DPR was created by law on 9 October 2007. It is composed of four Members of Parliament and four members of the Senate. It is tasked with controlling the government's policy and actions regarding intelligence.

440 LOI n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, Journal officiel, no. 0255, 31 October 2017. Available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000035932811, [Accessed 28 October 2025].

to security and public order. It authorised a prefect to order without any judiciary authorisation the visit to any location which is suspected of being visited or used by a suspected terrorist and the seizure of any document, object or data that would be retrieved during the visit.[441] It allowed the consultation of Air Transport Passenger Name Records. It created a distinct national database of Maritime Transport Passenger Names Records; and it authorised the unrestricted interception of radio communications.

Finally, on 30 July 2021, a law for the prevention of terrorist acts[442] authorised intelligence services to experiment until 31 July 2025, with the interception of satellite communications to prevent terrorist attacks and other significant attacks against public order. It also confirmed authorisation permitting the automated processing of connection and navigation data on the internet and extended it to URL addresses. It reinforced the prior control by the CNCTR over intelligence techniques; and streamlined the intelligence sharing procedure between services and between services and other administrative authorities.

As defined in a decree dated 12 May 2014[443] which was revised on 14 June 2017,[444] six services from the French administration are specifically specialised in intelligence. All are, therefore, tasked to search, collect, exploit and disseminate to the French government intelligence related to strategic and geopolitical interests, as well as to threats and risks that might affect the daily life of the Nation.

441 The authorisation to seize documents and objects was abrogated on 29 March 2018 by the Conseil Constitutionnel (Constitutional Council).

442 LOI n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, *Journal officiel*, no. 0176, 31 July 2021. Available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043876100, [Accessed 28 October 2025].

443 Décret n° 2014-474 du 12 mai 2014 pris pour l'application de l'article 6 nonies de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires et portant désignation des services spécialisés de renseignement, *Journal officiel*, no. 0111, 14 May 2014. Available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000028930926, [Accessed 28 October 2025].

444 Décret n° 2017-1095 du 14 juin 2017 relatif au coordonnateur national du renseignement et de la lutte contre le terrorisme, à la coordination nationale du renseignement et de la lutte contre le terrorisme et au centre national de contre-terrorisme, *Journal officiel*, no. 0139, 15 June 2017. Available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000034938469, [Accessed 28 October 2025].

These six services compose the 'first circle' of the French Intelligence Community (FIC)

La communauté française des services de renseignement, ©DRM

Three depend on the Ministry of Defence: the Direction Générale de la Sécurité Extérieure (DGSE – Directorate General of Foreign Security),[445] the Direction du Renseignement Militaire (DRM – Directorate of Military Intelligence)[446] and the DRSD (Direction du Renseignement et de la Sécurité de la Défense (DRSD – Defence Directorate of Security Intelligence).[447] One depends on the Ministry of Interior: the Direction Générale de la Sécurité Intérieure (DGSI – Directorate

445 Led by a Director General reporting directly to the Minister of Defence, the DGSE is France's only special service. It includes an armed clandestine branch and is tasked with collecting and exploiting intelligence relevant to national security, as well as detecting and countering espionage abroad against French interests. The DGSE was created by the 2 April 1982 decree. Its status and missions are defined in articles D.3126-1 to D.3126-4 of the Defence Code and its organisation is determined by the 13 July 2022 decree.

446 As the Intelligence Service from the Armed Forces, the DRM depends on the Joint Chief of Staff and provides the Chief with intelligence of 'military interest'. Created by the 16 June 1992 Decree, its missions are defined in articles D.3126-10 to D.3126-14 of the Defence Code and its organisation is determined by the 30 March 2016 decree, called in this case 'arrêté'.

447 The DRSD is at the direct disposal of the Minister of Defence to ensure the security of the Ministry of Defence (MoD)'s personnel, information, sensitive equipment and facilities. It is notably tasked with counter measures against terrorist, espionage, subversive, sabotage and organised crime activities. Its missions are defined in articles D.3126-5 to D.3126-9 of the Defence Code.

General of Domestic Security).[448] Two, meanwhile, depend on the Ministry of Finance: the Direction Nationale du Renseignement et des Enquêtes Douanières (DNRED – National Directorate for Customs Intelligence and Investigations)[449] and TRACFIN (Financial Intelligence and Investigations Service).[450]

If we consider law enforcement as the activity to prevent crime, responding to criminal complaints, investigating crimes, arresting suspected criminals and recovering stolen property, **only the DGSI has both intelligence and law enforcement prerogatives among the six services of the 'first circle'**.

Mr. Bernard Warusfeld, a scholar in Paris 8 University who moderated on 11 May 2023 the symposium titled 'Is the public policy on intelligence well overseen?'[451], organised at the National Assembly by the Délégation Parlementaire au Renseignement (DPR – Parliamentary Delegation on Intelligence), underlined that the DGSI is in a unique place. This service is both an intelligence and a judiciary-police organisation and is, therefore, under the legal framework applicable to intelligence techniques but also to the penal code of the judicial authorities.

The DGSI's website further indicates that, beside its intelligence gathering mission, the service is also a specialised judiciary police with a number of judiciary investigators. These are all qualified Agents or Officiers de Police Judiciaire (APJ / OPJ), specialising in terrorist litigation. The website describes a typical DGSI operation, starting from intelligence gathering *via* cyber-infiltration, followed by evidence gathering by judiciary investigators, tracking and, finally, the arrest of the suspects.

448 An active service of the National Police, the DGSI is active over all French territory and is tasked with collecting, centralising and exploiting intelligence related to national security of France's vital interests. The DGSI prevents and represses all kinds of foreign interference, terrorist acts, violent extremist individuals and groups, violations of national defence secrets, and attempts against the economical, industrial and scientific patrimony as well as activities linked to the acquisition or manufacture of weapons of mass destruction. It also monitors the activities of international criminal organisations which could have an impact on national security and prevents and represses criminal activities linked to information and communication technologies. The historical successor of the Direction de la Surveillance du Territoire (DST) and of the Direction Centrale du Renseignement Interieur (DCRI), was created by the 30 April 2014 decree, which also determines its missions.

449 The DNRED has a national competency, depends on the Directorate General of Customs and is tasked with customs intelligence. Created by the 1 March 1998 'arrêté', its missions and organisation are determined by the 29 October 2007 'arrêté'.

450 TRACFIN is the acronym for Traitement du Renseignement et de l'ACtion contre les circuits FINanciers clandestins (Intelligence procession and action against clandestine financial channels). Placed under the authority of the Ministry of Finances, one of its missions is to collect, assess and disseminate intelligence related to clandestine financial channels, money laundering and terrorism financing. Created by the 9 May 1990 decree, its missions are determined by articles R561-33 to R561-36 of the Monetary and Financial Code.

451 Assemblée nationale — Délégation parlementaire au renseignement, 2023. 'Les Actes du Colloque du 11 mai 2023, à l'Assemblée nationale, sur le thème : "La politique publique du renseignement est-elle bien contrôlée ?"' [online] 2 November 2023. *Rapport d'information* no. 1692. Available at: https://www.senat.fr/rap/r23-006/r23-006.html [Accessed 5 November 2025].

The judiciary investigators depend on the DGSI's Sous-Direction des Affaires Judiciaires (SDAJ – Sub Directorate for Judiciary Cases) which is under the authority of the Ministry of Justice's Parquet National Anti-Terroriste (PNAT – National Anti-Terrorist Prosecutor's Office). These investigators can conduct self-initiated investigations before any crime is committed in order to arrest and prosecute individuals planning violent actions on the national territory or intending to join foreign fighters' groups overseas. The DGSI's website underscores that the adaptation of intelligence into legal evidence acceptable in a court of law is one of the specific tasks of the SDAJ judiciary investigators.

Beside the services comprising the 'first circle', four additional intelligence services are part of what the French administration calls the 'second circle'[452] of the FIC. Two depend on the Ministry of Interior's Direction Générale de la Police Nationale (DGPN – Directorate General of National Police): the Direction Nationale du Renseignement Territorial (DNRT – National Directorate for Territorial Intelligence);[453] and the Direction du Renseignement de la Préfecture de Police de Paris (DRPP – Intelligence Directorate of the Paris Prefectorate).[454] One depends on the Ministry of Interior's Direction Générale de la Gendarmerie Nationale (DGGN – Directorate General of National Gendarmerie): the Sous-Direction à l'Anticipation Opérationnelle (SDAO – Sub Directorate for Operational Anticipation).[455] Finally, one depends on the Ministry of Justice's Administration Pénitentiaire (AP-Penitentiary Administration): the Service National du Renseignement Pénitentiaire (SNRP – National Service of Penitentiary Intelligence).[456] None of these four services has law enforcement powers and they are only tasked with gathering and processing intelligence for their respective administrations. They can however directly result in or influence law enforcement operations.

452 The 'second circle' comprises services or offices in which intelligence is one among other missions or intelligence services which belong to an administration with missions outside of the scope of intelligence.

453 The DNRT was created 29 June 2023 by decree 2023-530 and can use intelligence techniques in case of threat against national independence, national defence and the integrity of the French territory; prevention of terrorism; prevention of any attempt against the republican form of government; attempts to reconstitute dissolved groups; collective violent acts susceptible to seriously affect public peace; prevention of organised crime.

454 The DRPP was created by a 27 June 2008 'arrêté', which describes its missions. It depends on the *préfet* de Police de Paris (Paris prefect of Police) and is tasked with keeping him informed by collecting, centralising and analysing intelligence related to threats targeting the functioning of institutions, economic and social issues as well as violent urban phenomena in all domains related to public order enforcement. Its area of responsibility is Paris and the Hauts-de-Seine, Seine-Saint-Denis and Val-de-Marne *départements*. It assists the DGSI in preventing terrorist acts and in conducting surveillance operations targeting individuals, groups, organisations and societal phenomena liable due to their *modus operandi* to undermine national security. The DRPP can use intelligence techniques in the case of threats to national independence, national defence and the integrity of the national territory; prevention of terrorism; prevention of any attack on the republican form of government; attempts to reconstitute dissolved groups; collective violent acts susceptible to seriously affect public peace; and the prevention of organised crime.

455 Created by an 'arrêté' dated 6 December 2013, the SDAO is placed under the authority of the Director General of National Gendarmerie and provides intelligence related to national defence, national security and public order. It can use intelligence techniques in case of threat to national independence, national defence and the integrity of the national territory; for prevention of terrorism; attempts to reconstitute dissolved groups; collective violent acts liable to seriously affect public peace.

456 Created by an 'arrêté' dated 29 May 2019, the SNRP is active over the whole nation and is tasked with collecting, exploiting, analysing and disseminating information and intelligence likely to reveal serious attacks on France's fundamental interests, the security of penitentiary facilities and of health facilities which host detainees and penitentiary administration personnel.

For example, by providing intelligence to the Ministry of Interior on possible violence by extremist groups, a DNRT memo can decide a prefect to forbid or put limitations on a planned demonstration by citizens. Alternatively, the prefect might decide to deploy extra riot police alongside the demonstration's announced itinerary, with a risk of violent confrontation with extremists, leading to injuries and material damage, as well as to the arrest of suspects.

This is the same with the Gendarmerie's SDAO reports, which prefects may use, say, to justify classifying ecological demonstrations as potential disturbances and ordering their removal by riot gendarmerie and police units.

Regarding the SNRP, its specific task is to prevent escapes and to guarantee security and order in penitentiary units. The discovery through intelligence gathering of illicit equipment such as mobile phones in cells automatically results in a report to the judiciary authorities. This can result in search operations targeting detainees and their possible accomplices.

Apart from these four intelligence-dedicated services, the 'second circle' also comprises 22 law enforcement offices the principal task of which is not intelligence gathering. These offices comprise for example:

- the Counternarcotics Office of the Ministry of Interior's (MoI's) Direction Nationale de la Police Judiciaire (DNPJ – National Directorate of Judiciary Police).
- the Sub-Directorate for Counterterrorism of the MoI's DNPJ.
- the Anti-Cybercriminality Office of the MoI's DNPJ.
- the Office against Illicit trafficking of Migrants of the MoI's Direction Nationale de la Police aux Frontières (DNPAF – National Directorate of Border Police),
- the Sections de Recherche (SR – Research Platoons) of the French Gendarmerie.
- the Territorial, Interdepartmental and Departmental Directorates of the National Police.
- the Direction Régionale de la Police Judiciaire de la Préfecture de Police de Paris (DRPJP – Regional Directorate of the Paris Police Préfecture's Judiciary Police).
- the Direction de la Sécurité de Proximité de l'Agglomération de Paris (DSPAP – Directorate for Security and Community policing of the Paris Metropolitan Area).

As part of the 'second circle' these 22 offices and sub-directorates can proceed with intelligence techniques in case of any threat to national independence, national defence and the integrity of the national territory. They can also do so for the prevention of terrorism; in the case of any attack against the republican form of institution; to combat attempts to reconstitute dissolved groups; for the prevention of collective violent acts likely to seriously affect public peace; and, finally, for the prevention of organised crime.

3.4.2. Oversight and accountability mechanisms

Since 2007 which saw the creation of the DPR (Parliamentary Delegation on Intelligence), the French intelligence services and enforcement offices of the first and second circles of the FIC have been progressively subjected to a series of controls at different levels.

As described by the DGSI on its website, this agency is controlled:

- internally by its General Inspectorate.
- by the Ministry of Interior.
- by the Inspection des Services de Renseignement (ISR – Intelligence Services Inspectorate).[457]
- by independent administrative authorities such as the Commission Nationale de l'Informatique et des Libertés (CNIL – National Commission for Information Technology and Freedom).
- by the French legislative bodies via the DPR and the CNCTR for its use of intelligence techniques.

During her public intervention on the occasion of 11 May 2023 at a symposium 'Is the public policy on intelligence well overseen?',[458] Ms. Camille Hennetier, the then head of the SNRP, stated that her service was regularly subject to parliamentary, judicial, administrative and political control. Indeed, five checks had been carried out in 2022 by the CNCTR. The SNRP is also controlled by the Inspection Générale de la Justice (IGJ-Ministry of Justice General Inspectorate), the Inspection Générale des Affaires Sociales (IGAS-General Inspectorate of Social Affairs) and the Inspection des Services de Renseignement (ISR-Intelligence Services Inspectorate).

As part of the various checks exercised on the intelligence services, the 11 May 2023 symposium mentioned the DPR and the CNCTR as the two pillars of parliamentary oversight of the intelligence services. The CNCTR's pivotal role in protecting individual rights by advising the Prime Minister's Office on any request for the use of intelligence techniques was also emphasised.

457 Created by decree 2014-33 dated 24 July 2014 and placed under the direct authority of the Prime Minister the ISR is tasked to control, audit and advise the specialised intelligence services and the Intelligence Academy. The ISR checks that the intelligence services are law-abiding and follow ethical and deontological rules and that the operations they conduct are in accordance with the orientations determined by the National Council on Intelligence. By doing so, it contributes to the improvement of the performance of intelligence services.

458 Assemblée nationale — Délégation parlementaire au renseignement, 2023. 'Les Actes du Colloque du 11 mai 2023, à l'Assemblée nationale, sur le thème: "La politique publique du renseignement est-elle bien contrôlée ?"' [online] *Rapport d'information* no. 1692. Published 2 November 2023; deposited 4 October 2023. Available at: https://www.senat.fr/rap/r23-006/r23-006.html [Accessed 5 November 2025].

The then Director General of the DGSI, Nicolas Lerner, is currently the Director General of the DGSE. During the symposium he stated that due to the expertise developed within the service and the high-quality dialogue with the CNCTR, only a few intelligence technique requests were not authorised. Bertrand Chamoulaud, head of the SCRT explained that, despite the difficulties posed by the presence of 3000 agents in 99 departments who can request intelligence techniques authorisations, only 1 to 2% of these requests are rejected by the Prime Minister's office. This was, according to him, thanks to a permanent and confident dialogue with the CNCTR, and to the permanent training of the service's agents, which allowed the SCRT to create efficient internal structures capable of forwarding pertinent and adapted requests to the Prime Minister's Office, while respecting the legally-imposed frameworks.

Bertrand Chamoulaud also highlighted that all police officers and gendarmes belonging to the SCRT are committed to upholding the laws of the Republic and to enforce them. They are well-trained and fully aware that the intelligence techniques they are requesting go beyond standard law.

Serge Lasvignes, president of the CNCTR stated that in 2022, the intelligence services had sent 89,500 requests for the use of intelligence techniques targeting 21,000 individuals.[459] He indicated that there was no routine regarding surveillance, as the services regularly assess their requests and target new people, while stopping the monitoring of individuals who no longer represent a threat.

The CNCTR also proceeds to subsequent checks of intelligence collected by checking documents within the service's premises (121 such audits were conducted in 2022). There are also remote checks *via* dedicated computer applications.

According to Lasvignes, although the parliamentary control of Intelligence services is relatively recent in France in comparison with other western democracies, the CNCTR has been able to fully exercise its prerogatives. This is so even if it has limited resources compared to other countries. In fact, the nature and diversity of information it can have access to is sometimes envied abroad, as appears to be the case with their German Bundestag colleagues.

Lasvignes also declared he was very satisfied with the way CNCTR's recommendations were taken into account. The intelligence services carefully read its annual report, and they regularly report on the manner in which these recommendations are implemented.

459 The 'Vie Publique' website indicates that in 2022, 89,502 requests for the use of intelligence techniques were checked by the CNCTR, resulting in 20,958 individuals being subject to at least one intelligence technique, with 30% for terrorism prevention, 25% for organised crime prevention, 12% for prevention of attacks on the republican form of governments, attempts to reconstitute dissolved groups, and collective violence likely to seriously disturb public peace. Of the 89,502 requests, 629 were rejected by the CNCTR. Some of the rejected requests were linked to the prevention of collective violence, which according to the CNCTR, cannot limit the constitutional right to express one's opinions so long as the risk of a serious threat against public peace cannot be proven.

According to Title IV of the 24 July 2015 law on intelligence, any individual can petition the State Council (Conseil d'Etat) to know if he/she has been the subject of any kind of State Surveillance. To deal with these petitions, the Conseil d'Etat has had since 1 January 2016 a branch specialised in dealing with checking the CNCTR's decisions. According to its president, Rémy Schwartz, quoted in the 11 May 2023 symposium, this specialised branch has issued 516 decisions relating to petitions from citizens who consider that they are under surveillance.

The oversight of intelligence services with a law enforcement mission and law enforcement agencies allowed to use intelligence techniques, appears to have reached, since 2015, a level that is satisfactory to members of the parliament, as well as to the intelligence services. In the 2023 Symposium all parties acknowledge considerable progress, which, far from weakening the services, tends to strengthen them by allowing legislators to better know trends, threats and needs in an appropriate framework.

According to Member of the National Assembly Sacha Houlié, who presides over the DPR, 'the strength of our ties (with the intelligence services) and our mutual trust are enough to make our foreign colleagues jealous'.

François Noël Buffet, Member of the Senate and of the DPR, mentions 'a climate of trust between the DPR and the services', built overtime within the limits settled by law.[460] This is the most important result to achieve in relations between parliament and the FIC.

Bertrand Chamoulaud, head of the SCRT, explains that his service put in place, with the president of the CNCTR, a system 'based on exchange, trust and transparency, which aims to explain our needs and expectations, but also to improve the quality of our requests'. He mentions a 'constructive dialogue' with the DPR, the CNCTR, the ISR and other bodies.

Nicolas Lerner, the then Director General of the DGSI, also mentions the trust found within the CNCTR. There are very few refusals of requests for the use of intelligence techniques.

Serge Lasvignes, president of the CNCTR, confirms the excellent relations with the intelligence services, in particular with the DGSI and the SCRT, built, as he insists, on exchange and dialogue.

460 The law limits the need-to-know to past operations and the members of the DPR cannot be informed on ongoing operations in order to protect the agents and intelligence officers' security. However, the DPR can inspect stations overseas and have access to their documents as long as they are not linked to ongoing events.

However, there is still room for progress. The quick evolution of technologies, particularly in the information and communication domains, implies new needs and procedures for the intelligence services. This involves more and more sophisticated technical intelligence systems, that are more and more difficult to control.[461]

Another point where improvement is necessary is the audit of exchanges of information and data by the FIC's services with their foreign partners. This is a question rendered more complex by the absolute necessity for the intelligence services, and particularly the DGSE and the DGSI, to protect their sources.

Besides the official parliamentary oversight of internal and external controls by different administrative bodies, FIC' activities are regularly and independently scrutinised and reported on:

- By journalists specialised in defence and intelligence matters such as jean guisnel and dominique merchet who cultivate their own sources within the agencies or in their close circles and who dare to publish sometimes challenging articles targeting the fic.
- By confidential letters accessible online such as 'intelligence online'[462], which also have their own sources within or close to the fic and that do not hesitate to reveal information that could be controversial.
- Think tanks focused on geopolitical issues, with one specifically dedicated to intelligence called the cf2r (centre français de recherche sur le renseignement).[463] Cf2r focuses in developing a culture of intelligence among the general public.
- Former members of the intelligence community such as the presenter of the youtube channel 'talk with a spy'.
- Advocacy ngos such as amnesty international france, the league for human rights (ligue des droits de l'homme), reporters without borders and the quadrature of the net who protect the rights of citizens against potentially aggressive intelligence collection methods.

461 Patrick Pailloux, ex-Head of the Technical Directorate of the DGSE, suggested during the 2023 symposium that data experts and information technology technicians be recruited by the CNCTR to assist them in better assessing and controlling the intelligence techniques put in place by the services after the CNCTR approved their requests.

462 Intelligence Online, n.d. 'Home'. [online] Paris: Indigo Publications. Available at: https://www.intelligenceonline.com [Accessed 28 October 2025]. It is published in French and English.

463 Centre français de recherche sur le renseignement (CF2R), nd. 'Home'. [online] Paris. Available at: https://www.cf2r.org [Accessed 28 October 2025].

- Trade unions such as the judges trade union (syndicat de la magistrature) who are also focused on the protection of the rights of the citizens against potential fic abuses.

- And European bodies such as the European Union Agency for Fundamental Rights.

Whistleblowers, called in France 'lanceurs d'alerte', are protected by law. But the activities of the FIC, which are covered by the Secret de la Défense Nationale (French National Defence Secrecy law), are formerly excluded from the scope of that law. To the best of my knowledge, no whistleblower has until now been involved in any revelation linked to the FIC.

Revealing information protected by the 'Secret de la Défense Nationale' is punished by law. The pieces of information published by journalists and confidential letters are often considered as being covered by the law. Their publication can have serious consequences, which interfere with the freedom of the press and the rights of journalists.

This was the case in the spring of 2019, when six journalists investigating the use of French weapons systems in Yemen were summoned by the DGSI for having obtained and published extracts of a confidential note of the French Military Intelligence Directorate (DRM) related to that matter. The French media and the Journalists Trade Union mounted a campaign to publicise the investigation of their colleagues by the DGSI, and the six journalists were not, in the end, prosecuted.

Former members of the FIC – such as Olivier Mas, the presenter of 'Talks with a Spy'[464] – remain anonymous or use pseudonyms. They generally avoid revealing information that could be negative or compromising for their former service, and, when they do so, such as the late Pierre Siramy in his book *25 years in the Secret Services*, they are prosecuted and suffer financial penalties with suspended jail terms. In severe cases they can be stripped of their medals, awards, and commendations.[465]

NGOs, Trade Unions, Journalist Associations and European Associations aim at informing the general public in order to exert pressure and leverage on the parliamentarians of the National Assembly and the Senate, who include members of the Parliamentary Delegation for Intelligence. This is particularly important before a law is adopted.

464 Olivier Mas (his real identity remains concealed and Olivier Mas, who first appeared online as Beryl-614 is a pseudonym) is an ex-DGSE officer who served for fifteen years as a clandestine agent, a case officer and head of overseas stations. He has created his own channel on Youtube and has authored three books based on his experiences in the Service.

465 New cases like Syramy's recently emerged with, for example, the indictment in May 2024 of former DGSE Lieutenant-Colonel Lhuillier who published in 2023 his memoirs under the title *The Man of Tripoli*.

The July 2015 law on intelligence was the subject of a negative media campaign in the run up to its ratification. This included articles in the national financial newspaper *La Tribune*, famously read by decision makers in the economic and political sectors. But the real impact of such campaigns is not important since most of the French citizens either have a good opinion of their Intelligence Community or do not feel concerned by this topic which they consider far from their daily worries.

The French Republic is a very centralised state and, in line with the current constitution, the FIC is part of what the French political analysts call the 'reserved domain' of the President of the Republic. FIC enjoys a high level of confidentiality and is generally not overseen by any legislative or judicial body or by civil society.

The FIC's first circle heads of Agencies depend directly on the President of the Republic. This is so even if the official organisational charts put them under the responsibility of their respective ministers (Defence, Interior and Finance). Typically, each president, whatever his political orientations, has been extremely protective of his 'reserved domain'. Evidence of this can be found in the example given above of the summoning of journalists after the publication of extracts of the Military Intelligence note on the presence of French weapons systems used against Yemeni.

The lack of interest among the population in relation to defence matters adds to the difficulty of Civil Society Organisations in their oversight of the activities of the FIC. It makes CSOs vulnerable to prosecution by the Judiciary, who are confident in the lack of public engagement.

Whistleblowers cannot talk about events covered by the 'Secret de la Défense Nationale', but the French Journalists Trade Union is still influential enough for its journalists not to be prosecuted, even if summoned. They can still invoke the sacrosanct right to protect their sources, a right any prosecutor will hesitate to confront.

3.5. Lithuanian case study: Intelligence oversight model

Nortautas Statkus and Andrius Tekorius

3.5.1. Lithuanian intelligence services: Evolution, boundaries, and overlaps

Intelligence activities are traditionally classified into several domains: military and non-military intelligence, external intelligence, counter-intelligence, and criminal intelligence. This framework forms the foundation of the Lithuanian intelligence system, which has undergone significant structural and legal development, particularly since regaining independence.

The intelligence and security institutions of the Republic of Lithuania – the State Security Department and the Military Intelligence Institution – were re-established immediately after the declaration of independence of the Republic of Lithuania in 1990, reviving the functions of their predecessors that operated during the interwar period. These predecessors included the State Security Department (1923-1940) and the Intelligence Unit of the Lithuanian Armed Forces, which was established in 1918 as part of the Ministry of National Defence and that played a key role in military planning and counter-intelligence.

The State Security Department under the Government of the Republic of Lithuania was re-established on 26 March 1990. Over the following years, the institution underwent several name changes: in 1991, it became the National Security Service of the Republic of Lithuania; in 1992, it was renamed the Security Service of the Republic of Lithuania. Then, in 1994, following the adoption of the Law on the State Security Department of the Republic of Lithuania by the Seimas (the unicameral national legislature), the institution assumed its current name—the State Security Department (VSD).

At that time, the VSD's core functions encompassed intelligence, counter-intelligence, the protection of constitutional and economic foundations, as well as efforts to counter terrorism, serious organised crime, corruption, and smuggling. It was also tasked with the protection of state secrets, the safeguarding of government communications, and of conducting pre-trial investigations of crimes against the state. As such, the VSD combined intelligence and law enforcement functions.

The VSD operated under the legal framework established by the Law on the VSD, its Statute, the Criminal Code, the Code of Criminal Procedure, and other relevant legal acts.

The Military Intelligence institution was re-established shortly thereafter, on 1 June 1990, as the Intelligence Division within the Department of National Defence under the Government of the Republic of Lithuania. In 1992, it was reorganised into the 'A' Division of the Information Service of the Ministry of National Defence, then later into the Second Service, and ultimately, in 1993, into the Intelligence Department.

The military counter-intelligence structure was revived in 1991 as the Immunity Service of the Department of National Defence and was reorganised into the Counter-intelligence Department in 1992. In 1994, as part of a broader reform of military intelligence, the Intelligence Department and Counter-intelligence Department were merged into a single Intelligence and Counter-intelligence Department. This was, later that same year, renamed the Second Investigation Department (AOTD) under the Ministry of National Defence.

While military intelligence performed traditional intelligence functions, the military counter-intelligence component was responsible for counterespionage and for the protection of classified information in the field of national defence. The AOTD operated under its own Statute.

Both the VSD and the AOTD were also governed by broader legislation, including the Law on the National Security Framework, the Law on State and Official Secrets, the Law on Intelligence, and the Law on Operational Activities, in addition to other applicable legal acts. Note that the Law on Operational Activities regulated the activities of intelligence agencies and other criminal intelligence entities.

In 2013, Lithuania undertook a major reform of its intelligence system, aligning it with NATO and European Union intelligence standards and recommendations. The Lithuanian Parliament adopted a new Law on Intelligence, setting revised goals, functions, coordination mechanisms, and oversight procedures for the country's intelligence institutions. It also ensured equal social guarantees for intelligence officers and for employees of both intelligence institutions and codified the legal framework governing intelligence operations. The new law repealed the previous Law on the VSD, as well as the statutes of both the VSD and AOTD.

In the same year, the Law on Criminal Intelligence replaced the 1992 Law on Operational Activity. This established a new legal framework for the activities of all criminal intelligence entities in Lithuania, including the State Security Department (VSD) and the Second Investigation Department (AOTD), when conducting investigations into threats to state security—such as espionage, aiding foreign states acting against Lithuania, or breaches of classified information protection. As part of the broader intelligence system reform, the VSD was simultaneously relieved of its responsibilities for pre-trial investigations and the protection of

government communications. In this way the institutional boundaries of intelligence were clarified and overlapping law enforcement functions were eliminated.

The existing modern intelligence system emerged as part of broader efforts to build democratic institutions and align national security mechanisms with Euro-Atlantic standards. Two principal institutions, as designated by the Law on Intelligence, carry out core national security intelligence functions: the State Security Department of the Republic of Lithuania (VSD) and the Second Investigation Department under the Ministry of National Defence (AOTD). These bodies are entrusted with the dual functions of intelligence and counter-intelligence, which are vital to both internal and external threat mitigation.

In parallel, criminal intelligence—distinct from national security intelligence—plays an essential role in ensuring public safety and the effectiveness of law enforcement. Criminal intelligence activities are conducted by seven specialised institutions authorised under the Law on Criminal Intelligence: the Police Department, the Financial Crime Investigation Service (FNTT) and the State Border Guard Service (VSAT) under the Ministry of Interior, the Customs Department under the Ministry of Finance, the Special Investigation Service (STT), the Dignitary Protection Service (VST), and the Lithuanian Prison Service (LKT).

Each of these agencies is empowered to conduct intelligence within its legally assigned sphere, targeting threats such as organised and serious crime, corruption, financial offences, illegal migration, smuggling, and threats to the security of domestic and foreign dignitaries. Oversight of legality, however, is fragmented: while the Intelligence Ombudspersons oversees the VSD and AOTD, criminal intelligence institutions fall outside this mandate and are subject to different accountability frameworks—Lithuanian Prosecutor General's Office.

VSD is Lithuania's main non-military intelligence and security service, reporting directly to the Parliament of the Republic of Lithuania (Seimas) and the President of the Republic. This institution operates in the socio-political, economic, technological, and informational domains, excluding military-related fields. In addition to gathering strategic intelligence, the VSD is tasked with:

- Ensuring the security of diplomatic missions abroad (excluding military deployments).
- Protecting State and official secrets, apart from those managed by defence institutions.
- Overseeing the security of public administration communication systems, including cryptographic infrastructure.

A central function of the VSD is counter-intelligence—detecting and neutralising the activities of foreign intelligence services operating on Lithuanian territory. In this capacity, the VSD plays a critical role in protecting national sovereignty and the integrity of classified information.

The AOTD, under the Ministry of National Defence, is responsible for military intelligence and counter-intelligence. It conducts intelligence activities in areas such as:

- Military-political, military-economic, and military-technological domains.
- Support for defence planning and military operations, including those carried out abroad.
- Protection of defence-related classified information.

Its primary objective is to ensure early warning and strategic awareness to bolster Lithuania's defensive capabilities. Additionally, the AOTD plays an important role in international security cooperation, particularly by supporting NATO and EU missions.

While the division of responsibilities between VSD and AOTD is clearly defined in law, certain areas of activity—such as cyber threats, foreign influence, and hybrid threats—have introduced increasing functional overlaps. For instance, cyber-espionage operations can simultaneously target military systems (under AOTD's jurisdiction) and public-sector infrastructure (under VSD's remit). Coordination mechanisms are thus essential in avoiding duplication or gaps in coverage.

To maintain legal and operational coherence, the activities of all intelligence agencies are embedded in a comprehensive legal framework, including the:

- Constitution of the Republic of Lithuania.[466]
- Law on the Foundations of National Security.[467]
- Law on Intelligence.[468]
- Law on Criminal Intelligence.[469]
- Law on the Use of the Polygraph.[470]
- Law on State and Official Secrets.[471]
- Other national legislation and international obligations.

466 The Constitution of the Republic of Lithuania. n.d. *e-Seimas*. Available at: https://e-seimas.lrs.lt/portal/legalAct/lt. [Accessed 25 July 2025].

467 The Law on the Foundations of National Security of the Republic of Lithuania. n.d. *e-Seimas*. Available at: https://e-seimas.lrs.lt/portal/legalAct/lt. [Accessed 25 July 2025].

468 The Law on Intelligence of the Republic of Lithuania, n.d. *e-Seimas*. Available at: https://e-seimas.lrs.lt/portal/legalAct/lt. [Accessed 25 July 2025].

469 The Law on Criminal Intelligence of the Republic of Lithuania, n.d. *e-Seimas*. Available at: https://e-seimas.lrs.lt/portal/legalAct/lt. [Accessed 25 July 2025].

470 The Law on the Use of the Polygraph of the Republic of Lithuania, n.d. *e-Seimas*. Available at: https://e-seimas.lrs.lt/portal/legalAct/lt. [Accessed 25 July 2025].

471 The Law on State and Official Secrets of the Republic of Lithuania, n.d. *e-Seimas*. Available at: https://e-seimas.lrs.lt/portal/legalAct/lt. [Accessed 25 July 2025].

The Law on Intelligence sets out institutional mandates, rules for authorisation and operational conduct, and safeguards for the use and dissemination of intelligence information. Intelligence operations must adhere to general legal principles—legality, respect for human rights, public interest, accountability—and to specific principles tailored to the intelligence function, including political neutrality, confidentiality, timeliness, objectivity, and clarity.

Strategic coordination is overseen by the State Defence Council, chaired by the President of the Republic.[472] The Council defines annual intelligence priorities, based on which the Director of the State Security Department and the Minister of National Defence issue specific tasks to their respective services. The Council is also responsible for:

- Approving intelligence strategic guidelines.
- Evaluating the relevance and quality of intelligence products.
- Resolving jurisdictional overlaps where necessary.
- Recommending measures for greater operational synergy.

Although the institutional boundaries are legally established, the evolving nature of threats—from cyber-operations to disinformation campaigns—demands flexible, coordinated approaches. Effective cooperation and delineation of tasks between VSD, AOTD, and criminal intelligence agencies remain central to the integrity of Lithuania's national security architecture.

3.5.2. Oversight and accountability procedures

In Lithuania, as in other democratic societies, intelligence agencies are entrusted with broad and far-reaching powers—including access to classified information, surveillance capabilities, covert methods, and the ability to influence national security policy through the provision of intelligence assessments. While these powers are essential for addressing contemporary security threats such as espionage, terrorism, cybercrime, and foreign interference, their use must be carefully regulated and subjected to rigorous oversight to prevent abuse and maintain the public's trust. To guarantee both the legality and effectiveness of intelligence activities in Lithuania, a multi-layered oversight system is in place. This includes:

- Parliamentary oversight, primarily exercised by the Seimas Committee on National Security and Defence (NSGK), which monitors the strategic direction, accountability, and budgetary appropriateness of intelligence institutions.

472 The Law on the State Defence Council of the Republic of Lithuania, n.d. *e-Seimas*. Available at: https://e-seimas.lrs.lt/portal/legalAct/lt. [Accessed 25 July 2025].

- Judicial oversight, whereby certain intrusive intelligence methods—such as surveillance or interception—must receive prior authorisation by district courts, based on legal standards of necessity and proportionality—

- Executive control, exercised by the President of the Republic and the Government, mainly through the work of the State Defence Council, which defines intelligence priorities, evaluates performance, and ensures strategic coordination between agencies.

- Independent external oversight, entrusted to the Intelligence Ombudspersons, who monitor the legality of intelligence activities conducted by VSD and AOTD. These Ombudspersons operate autonomously and investigate complaints, systemic issues, and the lawfulness of internal practices.

- Additionally, data processing activities may be reviewed by the State Data Protection Inspectorate, which oversee implementation of GDPR, but not data processed for national security and defence purposes.

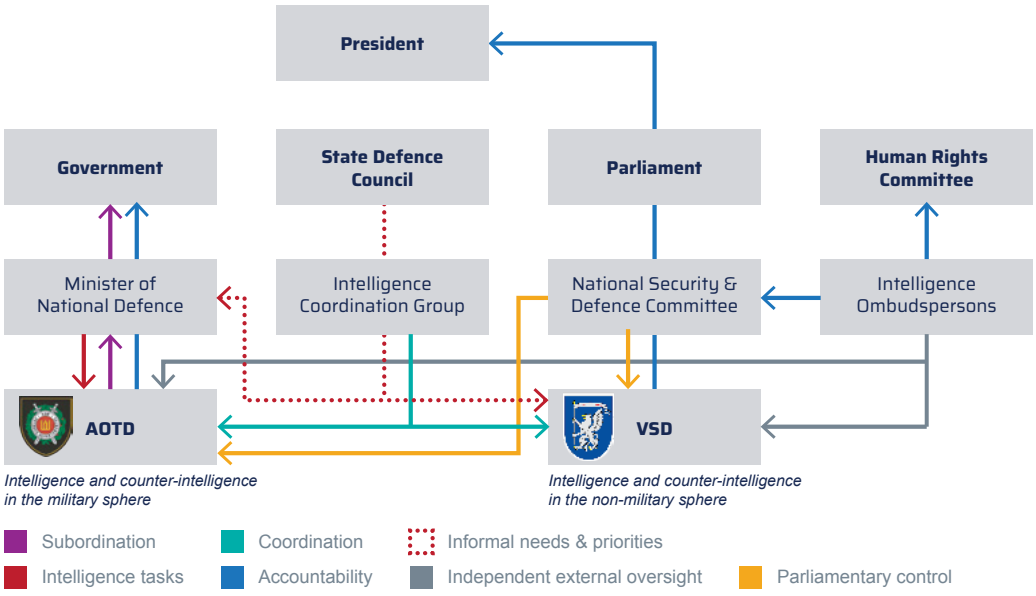
- In addition, the State Audit Office is responsible for supervising the financial operations of intelligence agencies.[473]

- Finally, to support accountability from within, the heads of Lithuanian intelligence agencies are legally required under the Law on Intelligence to establish robust internal control systems within their respective institutions. Directors have to ensure lawful, cost-effective, efficient, effective, and transparent activities of the agencies themselves.

This layered system of oversight reflects the principle that security and liberty are not mutually exclusive. Rather they must be balanced through transparent governance, institutional checks and balances, and adherence to the rule of law. Continuous evaluation and, where necessary, reform of oversight mechanisms are essential to maintain public trust and democratic accountability in the face of evolving threats and technological capabilities.

473 The Law on the National Audit Office of the Republic of Lithuania, n.d. *e-Seimas*. Available at: https://e-seimas.lrs.lt/portal/legalAct/lt. [Accessed 25 July 2025].

Figure 1. Control and Coordination of the Lithuanian Intelligence Agencies



3.5.2.1. Parliamentary Committees and Special Commissions: Ensuring legislative scrutiny

In Lithuania, the Seimas performs this oversight function primarily through NSGK. This standing committee is entrusted with comprehensive responsibilities in national security, intelligence, defence, and public order. It holds a permanent institutional role in evaluating the functioning of Lithuania's intelligence system and in assessing the adequacy of its legal and operational framework.

The role of the Committee on National Security and Defence

The NSGK has both legislative and supervisory powers. On the legislative side, it is involved in the drafting, review, and amendment of laws regulating intelligence activities, such as the Law on Intelligence, the Law on Criminal Intelligence, and the Law on the Intelligence Ombudspersons. The committee also considers appointments and accountability reports from the heads of intelligence agencies, assesses national threat assessments, and discusses strategic priorities defined by the State Defence Council.

In its oversight function, the committee:

- Monitors the implementation of intelligence mandates by the VSD and the AOTD.
- Reviews and assesses annual reports and briefings submitted by intelligence agencies.
- May conduct hearings, call intelligence officials to testify, and request classified briefings.
- Examines the budget allocations for intelligence services, contributing to financial transparency and efficiency.

Additionally, the NSGK serves as a forum for the public articulation of strategic risks, such as foreign interference, hybrid threats, and disinformation campaigns. Through its reports and recommendations, it influences national policy direction and serves as a bridge between the intelligence community and broader democratic society.

The interplay between Parliamentary and Independent oversight

The Seimas committee operates side-by-side with independent oversight bodies, such as the Intelligence Ombudspersons. Together these provide legal scrutiny of specific complaints, inspections and make sure internal practices comply with the Law. While the Ombudspersons focuses on individual rights and institutional legality, the Seimas exercises strategic, political, and structural scrutiny, ensuring that intelligence agencies:

- Serve national – not partisan – interests.
- Operate under a clear legal mandate.
- Maintain public legitimacy and respect for democratic principles.

This dual model reflects best practices across EU and NATO countries, where parliaments ensure political accountability, and in which independent oversight bodies monitor legal and human rights compliance.

Temporary and Special Parliamentary Commissions

In addition to standing committees, the Seimas has the constitutional authority to establish temporary parliamentary commissions or *ad hoc* inquiry bodies. These special commissions are formed to address specific incidents, allegations of misconduct, or to examine systemic failures within the intelligence or security sectors. While temporary in nature, such commissions may be granted extensive investigatory powers, including:

- Access to classified information (subject to applicable security procedures).
- The right to summon officials and other individuals to testify.
- The ability to produce public or classified reports containing findings and recommendations.

Parliamentary inquiries into intelligence services in Lithuania

2006: Temporary Parliamentary Commission on the Activities of the State Security Department

- **Context:** Public concerns emerged regarding the possible politicisation of VSD, alleged unlawful intelligence gathering on politicians, and potential leaks of classified information to the media.

- **Commission objective:** To determine whether VSD's activities were in line with the Constitution, the Law on Intelligence, and principles of human rights protection.

- **Findings:** The commission published a critical report, identifying systemic shortcomings and proposing directions for legal and institutional reforms. These had a direct impact on the reform of the VSD and the improvement of the legal framework.

  The Commission reached more specifically the following conclusions:

  1. The reorganisation of the VSD, the implementation of strategy, and the management and structural reforms were not progressing fast enough.

  2. a potential problem of politicisation of VSD officials was identified: some VSD investigations and actions of VSD officials may have been carried out or their results used for the benefit of certain political groups. In other cases, they may have been used for the benefit of the political groups themselves or for the benefit of politicians.

The Commission proposed to improve the legal regulation of the activities of the VSD:

- to regulate a clear procedure for the provision of information by the VSD to other state institutions.
- in the light of the experience of NATO and EU Member States, to provide an appropriate legal definition of the VSD's place among the institutions.
- to establish a more precise legal framework for parliamentary scrutiny of intelligence agencies.
- to regulate the possibility for intelligence officers to inform the parliamentary scrutiny bodies directly about problems in the service, without having to go through to their immediate superiors.
- to clearly regulate the procedure for the use and destruction of intelligence information.
- to provide for the possibility that a person receives information that intelligence actions have been carried out against him/her and regulate the procedure for appealing against such actions.

- **Significance:** This was the first case of formal parliamentary scrutiny over an intelligence service in Lithuania, setting a precedent for public accountability and oversight.

2009: Parliamentary Commission on the Possible Existence of CIA Detention Sites in Lithuania

- **Background:** International media reports, especially by *ABC News*, suggested that CIA-operated secret detention facilities may have existed in Lithuania, potentially with the cooperation of national security services.

- **Commission mandate:** To investigate whether Lithuanian intelligence services, particularly the VSD, were involved in unlawful detention or violation of international law.

- **Outcome:** The commission found insufficient evidence to confirm the operation of detention centres but acknowledged the existence of cooperation with U.S. intelligence counterparts.

  The Commission reached the following conclusions:

  1. The Commission did not establish whether persons detained by the CIA were transferred through the territory of the Republic of Lithuania or were brought to the territory of the Republic of Lithuania, but that the conditions for such transfer existed.

2. The Commission found that the VSD had received a request from its partners to set up premises in Lithuania suitable for holding a detainee, but that the premises were not used for that purpose.

3. The Commission found that, in the course of the VSD cooperation projects with partners, the heads of VSD at the time did not inform any of the country's top officials about the objectives and content of these projects.

Recommendations of the Commission:

1. Coordination and control of intelligence services should be strengthened by establishing a clear framework for identifying and assessing intelligence needs and priorities, the needs for international cooperation between intelligence services, and the tasks to be assigned to intelligence services, which also reflects institutional and political responsibilities.

2. The provision of information to the country's top officials must be improved. The procedure for providing information needs to be clearly defined.

3. The structure of the VSD performance reports should be revised and more detailed:

- The parliamentary scrutiny committee should receive more detailed information on the international cooperation of the VSD.
- The information provided on the international cooperation of the VSD should reflect the results of the joint operations or activities, their evaluation and the resources used in the process of such operations or activities.
- The parliamentary scrutiny committee should be informed annually about the restructuring of the VSD, the reform's impact on the efficiency of the institution's activities, the management and the use of the resources available.

4. It is necessary to address the issue of providing classified information to decision-makers in cases where the originator of the information is not only the VSD.

5. The provisions of the Law on Intelligence should be improved by regulating more precisely the cooperation of intelligence services with other state institutions.

6. VSD should strengthen the protection of classified information and improve the control mechanism for ongoing investigations.

- **International dimension:** This case prompted follow-up investigations by the Parliamentary Assembly of the Council of Europe, the United Nations, and the European Court of Human Rights (ECHR) in *Abu Zubaydah v. Lithuania*.

2017–2018: NSGK Inquiry into Improper Influence on Political Processes

- **Purpose:** Conducted by the Seimas Committee on National Security and Defence, this inquiry aimed to examine whether intelligence information was used for political purposes and to evaluate the interactions between business groups, politicians, and intelligence services.

- **Focus:** Particular attention was paid to the role of the VSD in sharing intelligence with political decision-makers and the risks this may pose to institutional independence and public trust.

  The parliamentary inquiry received information on the links between Lithuanian politicians and business representatives and individuals who may pose a threat to the interests of the state. There was also the question of their possible unlawful influence on the decision-making process of state institutions or their unlawful influence on some politicians and/or political processes.

  The Commission has made the following proposals:

  1. In accordance with the Law on the Protection of Objects of National Security Importance of the Republic of Lithuania, a screening would be initiated of the transactions concluded by undertakings of national security importance. This applies to undertakings classified in the first or second category, to ensure compliance with national security interests.

  2. Draft legislation to introduce the institution of civil confiscation, which would enable the confiscation of assets belonging to or associated with organised criminal groups, as well as assets acquired through corruption offences.

  3. To improve other provisions of the legislation relating to the activities of the Seimas Provisional Commissions of Inquiry defining liability for the violation of the Law on the Seimas Provisional Commissions of Inquiry and for non-compliance with the Commission's legitimate requests.

  4. To prepare legislation on the establishment of an independent oversight institute (the Intelligence Ombudsman) for intelligence and criminal intelligence entities.

- **Results:** The inquiry recommended regulating the handling of intelligence information, strengthening safeguards on political neutrality, and ensuring more transparent inter-institutional cooperation.

2024: Special Parliamentary Commission on the so called 'Whistleblower Case'

- **Trigger:** A high-profile whistleblower from within the intelligence community came forward with allegations of internal misconduct, concerning data processing, decision-making procedures, and potential violations of human rights.

- **Commission objective:** To assess not only the substance of the complaint but also the broader institutional practices and safeguards within intelligence services, particularly relating to internal transparency and protection of whistleblowers.

- **Scope:** The commission explored the internal culture of intelligence institutions, mechanisms for reporting abuses, and the effectiveness of legal oversight, including the role of the Intelligence Ombudspersons.

  The Commission noted that:

  1. The VSD Director assisted Gitanas Nausėda, a candidate in the 2019 presidential elections, by collecting intelligence information on the candidate's entourage (the members of his team, the members of his campaign staff, and supporters).

  2. When collecting intelligence information, VSD did not ensure the control of the legality of the collection and the use of such information: the intelligence task was not formulated in the prescribed manner; the assignment to collect the information was not formalised in accordance with the procedure laid down in the legislation; the information was not classified in the prescribed manner; and the procedures governing the work with human sources were violated.

  3. The whistleblower suffered for his whistleblowing: his right to leave was obstructed, his previously normal activity of attending meetings organised by the VSD leadership was restricted, reform of the VSD was initiated, which led to the abolition of the unit he headed, and he was forced to resign from the VSD.

  Following an investigation, the Commission proposed certain measures on Criminal Intelligence and Intelligence Control and on the protection of the rights of whistleblowers:

  1. To amend the Law on the Intelligence Ombudspersons to provide the Intelligence Ombudspersons with the rights and duties to oversee the legality of the activities of criminal intelligence institutions and to assess their compliance with the protection of human rights and freedoms;

2. In order to strengthen the parliamentary scrutiny of the VSD and the STT, a review of the legal framework for parliamentary scrutiny would be undertaken, ensuring that the intelligence and criminal intelligence institutions provided the Seimas with all the information necessary for parliamentary scrutiny;

3. The Ministry of Justice and the Law and Order Committee of the Seimas was to prepare and submit to the Seimas amendments to the law establishing stricter liability for violations of the rights of whistleblowers.

4. The Government should compensate the whistleblower for the material and non-material damages he had suffered.

Three of the four parliamentary inquiries were launched on the basis of intelligence officers' reports on possible illegal actions by the VSD. The Law on Intelligence Ombudspersons and the Law on the Protection of Whistleblowers of the Republic of Lithuania regulate the reporting of intelligence officers.[474]

The Law on the Protection of Whistleblowers establishes the rights and obligations of persons who report violations in the institutions. It also sets out the grounds and forms of their legal protection, as well as the measures for the protection, encouragement and assistance of such persons. This is to provide adequate opportunities for reporting violations of law that threaten or violate the public interest and to ensure the prevention, detection and prosecution of such violations.

On 6 June 2025, the Constitutional Court of the Republic of Lithuania ruled that both the establishment of a temporary parliamentary investigation commission based on information from a whistleblower at the State Security Department (VSD), and the later approval of that commission's findings, violated the Constitution.

Specifically, the Court declared:

1. The Seimas resolution of 31 October 2023, which created the commission to investigate possible unlawful collection and use of personal data, interference with intelligence and law enforcement institutions, influence on the 2019 presidential elections, illegal support to a political campaign, violations of whistleblower rights, and influence over sanctions on Belarus, was unconstitutional. It breached Articles 67 and 76 of the Constitution and the principles of responsible governance and the rule of law.

474 The Law on the Protection of Whistleblowers of the Republic of Lithuania, n.d. *e-Seimas*. Available at: https://e-seimas.lrs.lt/portal/legalAct/lt. [Accessed 25 July 2025].

2. The Seimas resolution of 4 June 2024, which approved the conclusions of that commission, also violated the constitutional principles of responsible governance and the rule of law.

The Constitutional Court emphasized that while the Seimas has the right to form investigatory commissions, such actions must respect constitutional boundaries, protect individual rights, and preserve the separation of powers and the independence of intelligence institutions[475].

Institutional takeaways

The Seimas has repeatedly used temporary and special commissions as a mechanism to:

- Ensure the legal compliance of intelligence institutions.
- Investigate allegations of abuse of power or politicisation.
- Reinforce democratic transparency and accountability in matters involving classified operations.

The Seimas forms temporary parliamentary inquiry commissions (LTKs) even though it has a standing NSGK. This is primarily due to differences in mandate, legitimacy, and investigative power. While the NSGK conducts routine oversight of intelligence and security institutions, it lacks the enhanced investigatory powers granted to LTKs. For instance, LTKs can summon witnesses, demand classified documents and hold public or closed hearings. Assigning NSGK an LTK status allows it to temporarily operate with these elevated powers.

Moreover, LTKs are perceived as being more politically balanced and legitimate in politically sensitive cases, since their composition reflects the proportional representation of all Seimas factions and often includes opposition voices. This helps reduce perceptions of bias that may arise if only the NSGK—often aligned with the ruling majority—handles the matter. LTKs are also more visible and politically accountable, functioning as *ad hoc* instruments to address urgent public controversies or potential abuses of power that transcend routine oversight.

Members of these commissions are elected by the Seimas and typically drawn from various factions, ensuring political pluralism. While formally intended to be objective, the actual performance of LTKs varies; their findings are often shaped by political dynamics, with some commissions serving more as platforms for political accountability than neutral fact-finding bodies. Nonetheless, LTKs play a crucial

475 Lietuvos Respublikos Konstitucinis Teismas, 2025. Dėl Seimo laikinosios tyrimo komisijos, tyrusios galimą neteisėtą poveikį 2019 m. Respublikos Prezidento rinkimams, sudarymo ir jos išvados patvirtinimo, nutarimas, 6 June. Available at: https://lrkt.lt/lt/teismo-aktai/paieska/135/ta3138/content. [Accessed 25 July 2025].

role in upholding democratic oversight, especially in matters where the integrity of permanent structures like NSGK can be questioned.

These inquiries demonstrate Lithuania's evolving commitment to democratic intelligence oversight and illustrate how parliamentary institutions can act as guardians of legality, civil liberties, and institutional balance, even in highly sensitive national security contexts. However, their effectiveness has varied in practice. Some commissions have yielded meaningful scrutiny and public accountability, while others have struggled with political polarization, limited access to classified information, and inconclusive results.

3.5.2.2. Judicial oversight

The collection, processing, and analysis of intelligence information in Lithuania rely on a wide array of methods and technologies, including the use of advanced digital tools and, increasingly, artificial intelligence systems. The effectiveness of these operations hinges not only on the speed and accuracy of information processing. They also depend on the legality and proportionality of the methods applied. In democratic societies, where national security must coexist with fundamental human rights, judicial oversight serves as a cornerstone of accountability and legitimacy in intelligence-led activities.

However, in Lithuania, there are no specialized courts exclusively tasked with intelligence matters. Instead, intelligence-related cases—such as requests for covert action—are adjudicated by judges in general jurisdiction courts at the district level.

Intelligence collection in Lithuania is regulated by law. Agencies may gather data through several channels:

- Court-approved (sanctioned) actions.
- Access to public or State-run registers and databases.
- Cooperation with private legal entities or individuals.
- Application of intelligence methods regulated by Government resolution.

Intelligence agencies frequently combine multiple techniques to enhance data reliability and comprehensiveness.

Court-sanctioned measures and warrant regime

Among the most intrusive intelligence-gathering activities are those that require prior authorisation by a court. These include:

- Monitoring and intercepting electronic communications (including content and metadata).
- Secret surveillance and inspection of private premises or vehicles.
- Covert collection and inspection of correspondence, documents and items.
- Access to personal financial transactions and bank data.
- Retrieval of individual communications data from service providers.

Such measures constitute a serious interference with the right to privacy, and thus must be authorised through judicial warrants issued by competent courts. In Lithuania, the District Courts are typically tasked with evaluating intelligence agency requests for intrusive intelligence-gathering actions. Courts must assess:

- The legal basis for the request.
- The necessity and proportionality of the proposed measure.
- The specificity and credibility of the threat or intelligence objective.

This process ensures that intelligence agencies cannot act arbitrarily or excessively in their operations and that checks and balances are in place to guard against the abuse of power.

Criminal intelligence and counter-intelligence overlaps

In counter-intelligence operations, intelligence services such as VSD and AOTD are additionally authorised to apply selected methods from the criminal intelligence toolkit, as defined in the Law on Criminal Intelligence. These include:

- Covert human intelligence operations.
- Operational inquiries and interviews.
- Surveillance of persons, premises, or vehicles.
- Sting operations and stakeouts.

While such overlaps are legally permitted, they raise complex oversight challenges due to the convergence of security-based intelligence and law enforcement investigative practices. Notably, while criminal intelligence institutions (such as the Criminal Police or Financial Crime Investigation Service) are subject to prosecutorial and judicial control, national intelligence agencies fall under the supervision of the Intelligence Ombudspersons and, for covert actions, District Courts.

Cooperation between criminal intelligence bodies and national intelligence services in Lithuania is structured through formal coordination mechanisms.

These institutions operate under distinct legal mandates: criminal intelligence focusing primarily on preventing and investigating serious crimes, and national intelligence on broader threats to national security. They do, however, exchange information and provide mutual assistance within the boundaries of their respective competencies. This collaboration is particularly relevant in areas where criminal and national security threats intersect, such as terrorism, organized crime, and cyber threats. Coordination is facilitated through inter-agency working groups, joint task forces, and information-sharing platforms, ensuring that intelligence flows efficiently while respecting legal mandates and operational autonomy.[476]

Because intelligence operations often entail intrusions into fundamental rights, especially the right to privacy, freedom of correspondence, and protection of personal data, Lithuanian law imposes strict safeguards.

In accordance with the Constitution of the Republic of Lithuania, the European Convention on Human Rights, and relevant jurisprudence of the European Court of Human Rights, such intrusions are only permitted when the following criteria are met:

1. **Lawfulness:** The measure must be based on clear legal provisions.

2. **Legitimacy:** The objective pursued must be tied to a pressing public interest, such as national security, public safety, or the prevention of serious crime.

3. **Necessity and proportionality:** The intrusion must be suitable, least restrictive, and strictly necessary in a democratic society.

While the requirement of a statutory basis is typically clear and objective, the assessments of necessity and proportionality require careful contextual analysis. These involve value judgments by courts, prosecutors, and increasingly, by independent oversight bodies and national human rights institutions.

3.5.2.3. The role of Ombudspersons

Recently, Lithuania has joined many EU and NATO countries in advancing the protection of human rights and freedoms, as well as enhancing the oversight of intelligence and security agencies. Lithuania was the second-to-last to establish this kind of institution in the European Union. But it was not the last to start operating.

The Lithuanian Parliament has taken deliberate steps to establish an active Intelligence Ombudspersons. This institution is tasked with overseeing the legality

476 State Security Department of Lithuania (VSD), n.d. 'Intelligence and counter-intelligence'. Available at: https://www.vsd.lt/en/activities/intelligence/?utm_source; Valstybės saugumo departamentas (VSD), 2023. Ataskaita už 2022 metus [Annual Report for 2022]. 6–7. Available at: https://www.vsd.lt/wp-content/uploads/2023/04/VSD_Ataskaita_2023_04_19.pdf. [Accessed 25 July 2025].

of intelligence agency activities and assessing their compliance with human rights and freedoms protections.

Law on the Intelligence Ombudspersons has been adopted on 23 December 2021 by which an independent specialised control institution, tasked with ensuring control over the activities of intelligence institutions was established. The idea was that when performing the special functions assigned to intelligence services, those institutions would comply with the imperatives arising from the constitutional principle of a state under the rule of law. Crucially, they would not violate human rights and freedoms.

The Intelligence Ombudsperson is appointed by the Seimas for a term of five years, based on a nomination submitted by the Speaker of the Seimas. The same individual may not be appointed for more than two consecutive terms. To be eligible for this position, a candidate must be a citizen of the Republic of Lithuania, of good repute, hold a university Master's degree, and have at least ten years of professional experience in national security and defence or in the protection of human rights. Additionally, a valid Personnel Security Clearance granting access to information classified at the 'TOP SECRET' level is required. On 6 April 2023, the first Intelligence Ombudsperson was appointed by the Seimas as the Intelligence Ombudsperson and Head of the Intelligence Ombudspersons' Office. Dr. Nortautas Statkus is a seasoned professional with more than twenty years of experience in national security, foreign affairs, and public administration. He has held high-level leadership and advisory roles across key sectors of government, demonstrating the strategic insight and competence essential for the position.

Within this European oversight landscape, Lithuania's Intelligence Ombudspersons' Office bears close resemblance—in terms of mandate scope and appointment process – to bodies in neighbouring countries. Consider Norway's Parliamentary Oversight Committee, Portugal's Council for Oversight of the Intelligence System, Croatia's Council for Civilian Oversight, Belgium's Standing Committee R, the Netherlands' Review Committee on the Intelligence and Security Services, and Finland's Intelligence Ombudsman.

Mandate and functions of the Lithuanian intelligence Ombudspersons

The Intelligence Ombudspersons occupy a unique and independent position within Lithuania's multi-layered system of intelligence oversight. Their primary responsibilities include:

- Assessing the compliance of intelligence agencies' activities, decisions, and internal statutes with applicable laws, regulations, and human rights standards.
- Conducting inspections and investigations into potential violations of law or human rights by intelligence agencies or their officers.
- Examining complaints and reports regarding potentially unlawful or inappropriate actions by intelligence agencies or intelligence personnel.

To be in conformity with their mandate, the Intelligence Ombudspersons may initiate inspections – scheduled, unscheduled, or follow-up – to establish whether the conduct and decisions of intelligence agencies comply with legal requirements.

The use of 'unscheduled' inspections by the Intelligence Ombudsperson in Lithuania has proven to be a flexible oversight tool. While the term 'unscheduled' may not always be explicitly used, in practice, a large portion of inspections—particularly those based on complaints or urgent requests—are conducted without prior notice to the intelligence institutions.

A notable example in 2023 involved an inspection carried out at the request of the Temporary Inquiry Commission of the Seimas. The Ombudsperson conducted an inspection that included site visits related to the verification of data. The inspection was carried out promptly, allowing the Ombudsperson to gather independent information directly from the institution and to provide the Inquiry Commission with responses to all the questions posed, to the extent permitted by law and the applicable statutory procedures.

All complaint-based inspections can be considered unscheduled. When a complaint is received, the Ombudsperson has the authority to initiate on-site inspections without informing the institution in advance. These visits typically involve access to classified documents, interviews with staff, and review of internal procedures. After each inspection, a formal report is issued with findings and recommendations.

Investigations may be launched on their own initiative, especially where there are indications of power abuse, violations of rights and freedoms, or improper processing of sensitive data related to national security or defence.

Powers and access to classified information

During inspections and investigations, the Intelligence Ombudspersons—and staff members of the Intelligence Ombudspersons' Office authorised to assist them—are entitled to:

- Access State or official secret information, provided they hold the appropriate clearance (up to "Top Secret").
- Receive documents necessary for the investigation (excluding information about covert sources, classified intelligence personnel, or data from foreign partners).
- Enter the premises of intelligence agencies and request explanations from officers or individuals involved in the matter.
- Review court authorisations for intelligence gathering methods, though they do not evaluate the factual basis or legality of judicial rulings.

Although the Ombudspersons do not possess formal subpoena powers, they are entitled to request and receive written and oral explanations from intelligence officers and other individuals relevant to an inquiry. This procedural tool, while less coercive than a subpoena, enables the Ombudspersons to gather the necessary information to assess the lawfulness and proportionality of intelligence activities. The institution's effectiveness, therefore, relies not only on legal authority, but also on institutional access, cooperation practices, and the political culture of accountability.

Importantly, the Ombudspersons and their staff are bound by law to maintain the confidentiality of State, official, commercial, banking, and professional secrets.

Complaints, investigations, and mediation

An investigation may be initiated by:

- A complaint submitted by an individual or legal entity.
- A report from an intelligence officer.
- The Ombudsperson's own decision, based on preliminary indications of misconduct.

All complaints and reports are first assessed to determine whether they fall within the Intelligence Ombudspersons' legal mandate. If the matter is deemed to be within their competence, the Ombudsperson may initiate an investigation. If not, the complaint is dismissed, and the complainant is provided with a written explanation outlining the legal reasons for non-admissibility. This ensures that the institution's limited investigatory resources are focused on issues clearly falling under its jurisdiction, while also maintaining transparency and accountability in decision-making.

The Ombudsperson may also initiate a mediation process, as provided by Article 21 of the Law on Intelligence Ombudspersons. Mediation is a traditional ombudsperson tool aimed at resolving disputes swiftly and informally by encouraging voluntary corrective action. If mediation is unsuccessful, the complaint proceeds to a full legal and factual investigation.

The decisions adopted by the Intelligence Ombudspersons are advisory in nature. They do not possess the authority to issue binding rulings or to grant remedies that would directly affect the complainant's legal position. However, their findings are communicated to all relevant parties, including complainants, reporting officers, the heads of investigated intelligence agencies, and—in certain cases—other governmental or parliamentary bodies. Intelligence agencies are supposed to take into account the recommendations made by the Intelligence Ombudsperson and report on their implementation.

Under its statutory mandate, the Intelligence Ombudsperson is authorised to submit proposals to the President of the Republic, the Seimas, the Government, and other state institutions and agencies. These proposals regard the improvement of legal acts the regulation of activities of intelligence institutions, the protection of human rights and fundamental freedoms, and the safeguarding of personal data processed for the purposes of national security or defence. In addition, the Ombudsperson is empowered to inform the aforementioned authorities of any identified violations of laws or other legal provisions.

For instance, in 2023, with the aim of ensuring more effective protection of human rights and freedoms and introducing greater legal clarity in the regulation of intelligence operations, the Intelligence Ombudspersons' Office submitted a package of legislative proposals. These proposals targeted amendments to Articles 5, 11, 12, 16, and 24 of the *Law on Intelligence*, Articles 26 and 28 of the *Law on the Intelligence Ombudspersons*, and Article 22 of the *Law on Criminal Intelligence*. They were formally presented to the Seimas Committee on National Security and Defence and the Seimas Commission for Parliamentary Control of Criminal Intelligence.

Recognising the need to align legal norms with publicly accessible information on intelligence methods—as published by Lithuanian intelligence authorities themselves—[477] the Ombudspersons' Office recommended that the Seimas cease classifying intelligence methods *per se* as either classified or declassified. Nevertheless, it was simultaneously proposed that the procedures and conditions governing the application of such methods should remain classified in order to maintain operational security. Further proposals were directed at intelligence measures that do not require prior judicial authorisation yet that significantly infringe on individuals' privacy. The objective was to institutionalise human rights

477 Ministry of National Defence of the Republic of Lithuania, 2023. *Intelligence*. Available at: https://kam.lt/zvalgyba/. [Accessed 25 July 2025].

safeguards through clearer statutory standards. The core recommendations were as follows:

1. **Legal Anchoring of Intelligence Priorities:** Intelligence and counter-intelligence operations should be conducted on the basis of intelligence priorities and needs formally adopted at least annually and approved by the State Defence Council. These should serve as the legal foundation for all operational tasks. Introducing such temporal and procedural constraints would set explicit limits on the duration of extrajudicial surveillance and contribute to legal predictability and rights protection.

2. **Temporal Limitations on the Use of Intelligence Methods:** It was recommended that intelligence methods may not be used beyond the timeframe of the authorised intelligence task. This measure would ensure that any application of intrusive techniques remains tied to a specific operational mandate, thus limiting scope creep and potential misuse.

3. **Retention Periods for Intelligence Data:** To protect personal data and ensure proportionality, it was proposed to define explicit retention limits for intelligence information. The law should provide that such data may be stored only as long as is necessary to fulfil legitimate intelligence or counter-intelligence functions.

4. **Institutional Mechanisms for Human Rights Monitoring:** Finally, it was recommended to establish either a dedicated human rights evaluation unit within each intelligence institution or to appoint a designated officer responsible for assessing compliance with human rights standards. This would embed ongoing oversight mechanisms within intelligence structures themselves[478].

These proposals were taken into account during the 2024–2025 deliberations on amendments to the Law on Intelligence and contributed to the refinement of the regulatory framework governing intelligence practices in Lithuania.

Procedural guarantees and limitations

The Law on Intelligence Ombudspersons sets a one-year time limit for the submission of complaints or reports from the date of the contested action or decision. Complaints submitted after this deadline—or those that are anonymous or duplicative—are generally inadmissible, unless new evidence emerges or the Ombudsperson determines that an exception is warranted in the public interest.

478 Republic of Lithuania, 2000. *Law on Intelligence, No. VIII-1861, 25 January*; consolidated version. Available at: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.106097/asr [Accessed 25 July 2025].

A complaint or report may also be dismissed within ten working days if:

- It falls outside the legal remit of the Ombudsperson (for example, when complaining about unlawful actions by criminal intelligence entities or violations of children's rights).
- The issue is pending before a court or under review by another competent authority.
- A pre-trial investigation has been launched into the same subject matter.

All parties are duly informed of refusals and the legal reasons behind them.

Strengthening human rights protection and institutional trust

The Intelligence Ombudspersons play a critical role in safeguarding human rights and freedoms in the context of intelligence operations. By conducting independent investigations, hearing complaints, initiating inspections, and mediating disputes, they help ensure that the activities of intelligence agencies do not undermine democratic values or constitutional principles.

3.5.3. Conclusion

In Lithuania, a pluralistic and institutionalised system of oversight is vital for balancing national security imperatives with constitutional rights and democratic accountability. This framework reflects a shared legal and ethical understanding: intelligence powers must never be absolute, and the rule of law must prevail even in the realms of secrecy and security.

Historically, prior to the establishment of the Intelligence Ombudspersons institution in 2021, one of the key external oversight bodies for intelligence activities was the Parliamentary Ombudspersons. The Law on Intelligence of the Republic of Lithuania explicitly provided that complaints concerning alleged violations of human rights and freedoms by intelligence officers, in the course of conducting intelligence and counter-intelligence operations, were to be investigated by the Parliamentary Ombudspersons in accordance with the procedure laid down in the Law on the Seimas Ombudspersons.

However, the legal framework granted the Seimas Ombudspersons only an indirect and limited mandate in the field of intelligence oversight. Article 11 of the Law on the Seimas Ombudspersons required the submission and review of the part of their annual report relating to intelligence institutions by a parliamentary committee. In the absence of specific provisions defining their competence, the Ombudspersons' ability to assess intelligence officers' actions through the lens of human rights protection remained narrow in scope.

Recognising these structural limitations, the Seimas Ombudspersons themselves noted in their 2020 report that external oversight of intelligence institutions failed to cover all aspects of their operations. They specifically emphasised the unique nature and privileged legal status of the VSD, which, due to the sensitive and intrusive nature of its functions, poses a heightened risk to fundamental rights. In this context, it was deemed inappropriate to grant such an institution full autonomy without a dedicated and effective mechanism of external control.[479]

This acknowledgement laid the foundation for the establishment of the Intelligence Ombudspersons institution. After nearly two years of practical experience in supervising the legality of intelligence operations and ensuring their compliance with fundamental rights, the Intelligence Ombudsperson identified multiple gaps and inconsistencies in the legal framework that hinder effective oversight.

To address these challenges, the institution submitted a package of legislative proposals to the Seimas, targeting amendments to several articles of three key laws: the Law on Intelligence Ombudspersons, the Law on Intelligence, and the Law on Criminal Intelligence. These proposals aim to eliminate contradictions and ambiguities in the existing legal provisions, and to provide a more coherent, enforceable, and transparent oversight regime.

Legislative proposals were elaborated within the 2024 assessment of the legality of intelligence institutions' activities and their compliance with the protection of human rights and freedoms. This assessment, together with the annual activity report of the Intelligence Ombudspersons' Office, was presented to the Seimas Committees on National Security and Defence and on Human Rights and was published on the website of the Intelligence Ombudspersons' Office.[480]

On 13 May 2025, a draft Law on Intelligence Ombudspersons and accompanying legislative proposals—XVP-422 to XVP-424—were registered: the draft Law on Intelligence Ombudspersons, the draft Law on Intelligence, and the draft Law on Criminal Intelligence.[481]

The proposed legislative amendments would allow for the assessment of the legality of intelligence activities at the very outset of their implementation and ensure that human rights are not restricted unlawfully or without justification.

479 Seimo kontrolierių įstaiga, n.d. Seimo kontrolierių metinės veiklos ataskaita už 2020 metus. 21. Available at: https://www.lrski.lt/veiklos-sritys/metines-seimo-kontrolieriu-veiklos-ataskaitos/. [Accessed 25 July 2025].

480 Intelligence Ombudspersons' Office of the Republic of Lithuania (2024) Annual assessment of the legality of intelligence institutions' activities and compliance with the protection of human rights and freedoms. Available at: https://www.zki.lt/en/annual-assessments/. [Accessed 5 November 2025]

481 Seimas of the Republic of Lithuania, n.d. *Draft Law on Intelligence Ombudspersons and Related Bills (XVP-422–XVP-424)*. Available at: https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/b571dd82f31e11eea51cc3d8eb2f3837. [Accessed 25 July 2025].

Among the most important objectives is the refinement of terminology used in the laws, clarification of the Intelligence Ombudspersons' powers and functions, and the prevention of divergent interpretations in practical application. The proposals also seek to fulfil the original legislative intent behind the creation of this oversight institution. They ensure meaningful, independent oversight of intelligence bodies.

This is particularly important as the Seimas considers amendments to the Law on Intelligence that aim to expand the powers of intelligence institutions. These changes are set out in the draft law amending Articles 2, 5, 7, 9, 11, 13, 14, 18, 19, 24, 29, 33, 40, 43, 45, 49, 50, 55, 57, 60, 64, 64[1], 69, 70 and 71, and supplementing them with Annex 3 to the Republic of Lithuania's Law on Intelligence No. VIII-1861.[482]

To be effective, oversight must be grounded in robust legal authority and supported by unhindered access to all relevant information. It is, therefore, crucial to further define and expand the rights of Intelligence Ombudspersons to ensure continuous, independent, and proportionate monitoring of intelligence activities. This includes guaranteeing their ability to obtain all data necessary to perform their mandate effectively.

Lithuania's system of intelligence oversight is still evolving. The legal framework establishes clear mandates for parliamentary, executive, and independent oversight, and the creation of the Intelligence Ombudsperson institution marks a significant step toward institutionalizing accountability in a sensitive domain traditionally shielded from public scrutiny.

However, the effectiveness of this oversight depends less on the existence of laws and more on their practical enforcement, institutional capacities, and the political will to ensure transparency and control.

In sum, Lithuania's oversight system is a work in progress. It is grounded in law, driven by democratic intent, but still in need of structural reinforcement to fully live up to its potential.

482 Seimas of the Republic of Lithuania, n.d. *Draft Law Amending and Supplementing Articles of the Law on Intelligence No. VIII-1861*. Available at: https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/25804b30f3f311eea51cc3d8eb2f3837. [Accessed 25 July 2025].

3.6. Norwegian case study: Intelligence oversight

Henrik Gudmestad Magnusson

Information for this article was in part collected from the EOS Committee's annual reports[483] and information on the English version of the website.[484]

3.6.1. The EOS Committee as part of Parliament's external oversight

Oversight of intelligence and security services in Norway is performed by the Parliament Appointed Committee for Intelligence Oversight (the EOS Committee). The EOS Committee was established in 1996 after the end of the Cold War, following on from extensive public attention and political debate about the intelligence and security services. The decision to have one single oversight body was made in 1993. In 1996 an inquiry commission (the Lund Commission) uncovered unlawful registration and surveillance post 1945, especially of left-wing persons and organizations. This drove home the need for independent oversight. The public debate after the Lund Commission coincided with the first active year of the EOS Committee. The Lund Commission conducted a critical review of the past, while the EOS Committee sought to prevent mistakes from the past from being repeated.

The EOS Committee is a permanent oversight body appointed by Stortinget (the Norwegian parliament) whose task is to oversee Norwegian public entities that engage in intelligence and security activities. The Committee's work is regulated by the Act relating to the Oversight of Intelligence, Surveillance and Security Services (the Oversight Act). [485]

Oversight here is not limited to specific organisational entities. The main intelligence and security services in Norway are the Norwegian Police Security Service (PST), the Norwegian Intelligence Service (NIS), the Norwegian National Security Authority (NSM) and the Norwegian Armed Forces Security Department

483 EOS Committee, ND. 'Annual reports'. [online] Oslo. Available at: https://eos-utvalget.no/en/home/publications/annual-reports/ [Accessed 28 October 2025].

484 EOS Committee, ND. 'Home'. [online] Oslo: EOS Committee. Available at: https://eos-utvalget.no/en/home/ [Accessed 28 October 2025].

485 EOS Committee, 2025. *Annual Report 2024*. [online] Oslo: EOS Committee. Available at: https://eos-utvalget.no/wp-content/uploads/2025/06/EOS-annual-report-2024.pdf [Accessed 28 October 2025]. See Appendix Two for the English translation of the Act.

(FSA). But the Committee's remit also includes other parts of the Norwegian Armed Forces and government bodies such as the Civil Security Clearance Authority. The Committee may also conduct investigations into other parts of the Norwegian public administration that perform intelligence and/or security services. The Committee considers it a clear advantage to have one body to exercise democratic oversight over all Norwegian intelligence and security services. To be able to carry out comprehensive oversight is crucial in a time of increasing cooperation between services.

The Committee is independent of both the Storting and the government. However, the Storting may order the Committee to undertake specified investigations within the oversight remit of the Committee. In the first thirty years of the Committee's history the Storting has not made such a decision.

3.6.2. The purpose of the EOS Committee's oversight

The EOS Committee's oversight of the intelligence and security services is to ensure that said services are compliant with Norwegian laws and regulations. The Committee's remit does not include reviewing the services' effectiveness, how they prioritise their resources, or their budget.

The Oversight Act states three main purposes of the oversight:

1. To ascertain whether the rights of any person are violated and to prevent such violations, and to ensure that the means of intervention employed do not exceed those required under the circumstances, and that the services respect human rights.

2. To ensure that the activities do not unduly harm the interests of society.

3. To ensure that the activities are kept within the framework of statute law, administrative or military directives and non-statutory law.

The Committee's primary focus is to ensure that the services safeguard the security of individuals under the law, particularly in terms of protecting their civil liberties and guaranteeing due process in law. The Committee examines decisions made by the services to ensure that no individual has been subjected to unjust treatment and that the methods used are not more intrusive than necessary under the circumstances. The decisions are also examined to see if they are within the regulatory framework of the services.

Furthermore, the Committee is to see that activities carried out by the services in question do not unduly harm or impede the interests of Norwegian society.

3.6.3. Composition of the Committee and its Secretariat

The Committee has seven members. They are elected by the Storting for a term of up to four years. Members may be re-appointed once. No deputy members are appointed. Committee members cannot also be current members of the Storting, nor can they previously have worked in the intelligence or security services.

Much of the information handled by the Committee in its oversight activities is classified. Due to this, both the Committee members and the Secretariat are bound by a duty of secrecy. The committee members and secretariat employees must hold top-level security clearance and authorization. Of the seven Committee members, five have political backgrounds from different parties. The party groups are responsible for nominating candidates for the Committee to the Storting's presidium. The other two members are expert members, with professional backgrounds from the fields of law and technology.

The Committee enjoys a quorum whenever five members (a majority of four, plus one) are present. All members should be present for all Committee activities, but the Committee may split up during inspections of sites or local facilities.

The Secretariat has 30 employees. This includes the director of the Secretariat, two oversight departments and an administrative department. Staff members are allowed to have a background in the services.

Preparations and follow-up of internal Committee meetings and inspections are the main responsibility of the Secretariat. The Secretariat also assists the Committee in investigating complaints and cases raised on the Committee's own initiative. However, the final decision on any case is always taken by the Committee.

3.6.4. Access to information and limitations to the oversight

The Oversight Act grants the Committee access to the services' archives and registers. In its annual report for 2020 the Committee reflected on 25 years of oversight of the services and stated the following regarding access to information:

> *The Oversight Act in particular has proven to be effective when faced with services that have not always been obliging in relation to the Committee's requests for access to information. The right of inspection and access to information has been a vital prerequisite for the oversight – and for confidence in it. In light of regulatory changes as well as changes in what is technically possible, it is a continuous task for the Committee to make sure that the intelligence and security services facilitate our oversight.*

Access is not unlimited. The Storting has adopted a plenary decision that restricts the Committee's access to 'particularly sensitive' NIS 'information'.[486]

Apart from this, there are few limitations on the way the Committee performs oversight. By law the Committee is not to request access to classified information to a greater degree than is warranted by oversight purposes. Further, the Committee must take national security interests and the nation's relations with foreign states into consideration when performing oversight. The oversight shall also cause as little inconvenience as possible to the services' operational activities. A certain level of caution in overseeing the services is thus recommended.

The Committee is to follow the principle of subsequent oversight (*ex post*). However, the Committee may demand access to and comment on current issues.

The Committee's right to access information includes information held by government bodies and businesses that assist the services. The Committee can also summon employees of the services, other employees in the public administration and private persons to give oral evidence on specific matters.

There is a penal provision in the Oversight Act. Persons who do not facilitate for the EOS Committee's oversight in a manner that they have a legal obligation to do, can be sentenced to fines and a maximum of one year in prison. So far, the provision has never been used.

Oversight does not include activities involving persons who are not residing in Norway or organizations that have no address in that country. The same applies to activities involving foreign citizens whose residence in Norway is associated with service for a foreign state. However, the Committee may investigate these areas as well, if special circumstances so dictate. The decision on whether such circumstances are present is left to the Committee's discretion.

486 By 'particularly sensitive information', cf. the NIS's Guidelines for the processing of particularly sensitive information, is meant:

1. The identity of the human intelligence sources of the NIS and its foreign partners.
2. The identity of foreign partners' specially protected civil servants.
3. Persons with roles in and operational plans for occupational preparedness.
4. The NIS's and/or foreign partners' particularly sensitive intelligence operations abroad which, if they were to be compromised,
   a. could seriously damage the relationship with a foreign power due to the political risk involved in the operation, or
   b. could lead to serious injury to or loss of life of own personnel or third parties.

3.6.5. Inspections

A key part of the EOS Committee's activities is to carry out inspections of the intelligence and security services. By law the Committee is to inspect the headquarters of the PST at least twice a year, the NSM twice a year, the NIS twice a year, the FSA twice a year, the Norwegian Special Operations Command once a year and the Army Intelligence Regiment once a year. In addition, the local units of the services are also to be inspected regularly. The Committee is also to inspect police bodies and other bodies and institutions that assist the PST. This includes private firms. Other services may also be inspected, when it is relevant to the Committees area of oversight. The Committee also inspects the Civil Security Clearance Authority yearly.

Services are normally given prior notice of inspections, but the Committee may also carry out inspections unannounced. An unannounced inspection was part of the investigation that led to the special report in 2019 on PST's unlawful collection and storage of information about airline passengers.[487]

An inspection consists of a briefing and an inspection. The topics of the briefings are mostly selected by the Committee. The Committee is briefed about the services' ongoing activities, national and international cooperation, the use of intrusive methods, the processing of personal data and other topics. The services are also asked to brief the Committee on any matters they deem to be relevant to the oversight, including non-conformities that they themselves have identified. The Committee asks verbal questions during the briefings and sends written questions afterwards.

During the inspections, Committee members conduct searches directly in the services' systems. The services are not told which searches the Committee have carried out.

The Committee must adapt its oversight methods to technological development. In addition to inspections, the Secretariat conducts regular investigations of the services' systems. This enables the Committee to conduct more targeted and risk-based inspections.

For inspections of the PST, the Committee's main focus is the service's collection and processing of personal data, the use of coercive measures, such as wiretaps, and the exchange of information with domestic and foreign partners.

For NIS inspections, one of the primary concerns for the Committee is to make sure that the NIS abides by the provisions of the Intelligence Service Act. This

487 EOS Committee, 2019. *Special report to the Storting on PST's unlawful collection and storage of information about airline passengers*. [online] Oslo: EOS Committee. Available at: https://eos-utvalget.no/wp-content/uploads/2020/01/special-report-PST-airline-passenger-information-december-2019.pdf [Accessed 28 October 2025].

prohibits surveillance and/or covert procurement of information on Norwegians in Norway. Additionally, the Committee oversees the service's collection of information, the processing of personal data and the exchange of information with foreign and domestic partners. An important task for the Committee is to oversee a new method the 'facilitated collection of border crossing electronic communication'. This gives the NIS the possibility of tapping communications from fibre cables crossing the Norwegian border. The service needs court permission to make searches in the collected metadata and prior to the collection of content data.

When inspecting the NSM and the other security clearance authorities, the Committee focuses on the processing of and decisions in security clearance cases. During the inspections, the security clearance authority presents the Committee with a list of all complaint decisions where the complaint was denied. In addition, the Committee regularly carries out random checks of decisions to deny or revoke security clearance in cases where no complaint was lodged. The Committee also oversees NSM's other duties, its cooperation with other services and NCSC – the Norwegian National Cyber Security Centre.

Inspections of the FSA primarily focus on security clearance cases, but another key area of oversight is the FSA's responsibility for protective security activities in the Norwegian Armed Forces.

3.6.6. Statements

The Committee raises cases on its own initiative based on findings made during the inspections. Such cases may also be based on notifications the Committee receives or from public mention of a matter. To investigate a case, the Committee reviews documents from the service in question. The service must always be given the opportunity to state its written opinion on the issues raised in the case, before the Committee submits a statement that may result in criticism or other comments. Once concluded, the EOS Committee may express its written opinion on matters within the oversight area. Such opinions can be to criticise the service, to point out errors, to state that a decision is invalid or clearly unreasonable. The Committee can also ask the service to reconsider a matter or change internal practises. The Committee has noted that investigations that end with criticism are more often due to system errors than intentional acts.

The Committee's opinion is non-binding. The Committee cannot instruct the services or be consulted by them as part of their decision-making. Usually, the service will adhere to the Committee's decision in a case.

A certain threshold must be reached before the Committee is able to criticise the services' discretion in specific matters.

3.6.7. Handling of complaints

Complaints that fall within the EOS Committee's oversight area are investigated in the relevant service or services. The Committee has a low threshold for considering complaints. If the investigation of a complaint reveals grounds for criticism, this is indicated in a written statement to the service concerned. In such cases, the Committee may also ask the service to remedy the situation and follows up to check that they do so.

The Committee's statements to complainants should be as complete as possible but may not contain classified information. Both information that a person is being subjected to surveillance and information that a person is not being subjected to surveillance is classified information. If the Committee's investigation shows that the complainant's rights have been violated, the Committee may inform the complainant that the complaint contained valid grounds for criticism. If the Committee is of the opinion that a complainant should be given a more detailed explanation, the Committee may propose this to the service in question or to the responsible ministry. The service's or ministry's decision regarding classification of information is binding on the Committee and it is therefore prevented from informing the complainant about the basis for criticism without consent.

3.6.8. Reports to the Storting

The EOS Committee submits annual reports to the Storting about its activities. Special reports may also be submitted if matters are uncovered that should be made known to the Storting immediately. The Committee has so far issued twelve special reports.[488] Some examples are:

- Special report on the PST's registrations of persons connected to two Muslim communities (2013).
- Special report to the Storting concerning the legal basis for the Norwegian Intelligence Service's surveillance activities (2016).
- Special report to the Storting on PST's unlawful collection and storage of information about airline passengers (2019).

Both annual and special reports and their annexes shall be unclassified and are made available to the public. Before submitting the report to the Storting, the Committee confers with the services to ascertain whether certain information contained in the report is suitable for release.

488 EOS Committee, ND. 'Special reports'. [online] Oslo: EOS Committee. Available at: https://eos-utvalget.no/en/home/publications/special-reports/ [Accessed 28 October 2025]. Five of the special reports are translated into English.

The annual report includes an overview of the composition of the Committee, its meeting activities and expenses, a statement concerning inspections conducted and their results. Furthermore, annual reports contain an overview of complaints and what they resulted in, as well as a statement concerning cases and matters raised on the Committee's own initiative. If the Committee has requested measures be implemented within the services, it gives a statement in the annual report concerning these and what they have led to. Finally, the Committee can comment on its general experience of the services' activities, and on any need for regulatory changes.

The Committee's reports are given to the Storting's Presidium by the Committee Chair. The report is then assigned to the Standing Committee on Scrutiny and Constitutional Affairs. Most years the Committee presents the report in a meeting with the Standing Committee. The Standing Committee submits a written recommendation on the annual report to the Storting. The annual report is then debated in a plenary session in the Storting. Normally the ministers responsible for the services will attend the debate.

3.6.9. Oversight of law enforcement functions within the intelligence services[489]

The PST is Norway's domestic intelligence and security service. Its responsibilities include collecting and analysing information and implementing countermeasures against matters that threaten national security. This includes threats related to unlawful intelligence activities, extremism and terrorism, the proliferation of weapons of mass destruction, violations of export control and the Sanctions Act and sabotage. PST is organized as a special police service parallel to the regular police, but contrary to the regular police it reports directly to the Ministry of Justice and Public Security.

In Norway, law enforcement and intelligence are not separated within the security services. This means that PST conducts both preventive investigations and criminal investigations based on suspicions of criminal acts. The preventive activities are not considered criminal investigations and are conducted pursuant to the Police Act. In relation to the preventive activities, PST is subject to the authority of the Ministry of Justice and Public Security. These activities are fully subject to oversight by the EOS Committee.

489 Information for this section was, in part, collected from Mevik, L. and Huus-Hansen, H., 2007. 'Parliamentary Oversight of the Norwegian Secret and Intelligence Services'. In: H. Born and M. Caparini, eds. *Democratic Control of Intelligence Services: Containing Rogue Elephants*. Aldershot: Ashgate, 143–162.

PST activities, conducted as part of a criminal investigation, are regulated by the Criminal Procedure Act. PST has its own investigative unit together with its own prosecuting authority. These activities are subject to the powers of the superior prosecuting authority. In Norway the first level of the Prosecution Authority is part of the police. The Prosecution Authority in the Police is organised into twelve districts, the National Criminal Investigation Service and the PST.

The Prosecution Authority in the PST is organised directly under the National Authority for Prosecution of Organised and other Serious Crime, which is organised under the Director of Public Prosecution. The Prosecution Authority in the PST has the right to make prosecutorial decisions, such as whether a person is to be charged, the use of coercive measures and whether prosecution is recommended. The decision of whether to prosecute is made by the superior prosecuting authority. The Prosecution Authority in the PST can also be instructed by the superior prosecuting authority.

Oversight by the EOS Committee does not apply to the superior prosecuting authority, but it applies to the Prosecution Authority in the PST. The prosecuting authority in Norway has traditionally held an independent status as a guarantee against political pressure on prosecutorial decisions. This is why the superior prosecuting authority is exempt for oversight by the EOS Committee as a politically elected oversight body. The reason why the Prosecution Authority in the PST is not exempt from oversight by the EOS Committee, is that it would be difficult to draw a line between the investigative and the preventive activities in the PST. One case can start as preventive activities before it turns out that the inquiries lead to suspecting criminal acts and the start of an investigation. If the investigation does not lead to a criminal charge, the investigation case may be closed, but there might still be grounds to maintain the preventive case. It would be difficult for the EOS Committee to conduct effective oversight if only some of the circumstances or progress on a case can be examined.

Oversight of the prosecuting authority within the police is not as invasive for the prosecution's independence as it would be for the superior prosecuting authority. Therefore, the EOS Committee is conducting oversight both in investigative and preventive cases in the PST. However, the EOS Committee's oversight in the investigative cases could be difficult as there often will be extensive contact and cooperation between the responsible officer in the PST and the superior public prosecutor.

PST can use covert coercive measures and covert information collection methods in both preventive and criminal investigation. The use of covert coercive measures in the preventive cases is regulated by the Police Act, and their use in criminal cases is regulated by the Criminal Procedure Act. The EOS Committee shall oversee the use of covert coercive measures in both preventive and criminal cases. To use covert coercive measures PST needs a court order. The PST will specify the method they wish to use and why in their application to the court. The Court

will then decide and give a warrant for the method, a time period and any other conditions for the use of the method. The court's decisions are not subject to the EOS Committee's oversight, but the Committee will oversee that PST is using the measure in accordance with the court's instructions. The EOS Committee shall also examine whether PST gives all the relevant information to the court when they request for a coercive measure.

3.6.10. International oversight cooperation

The intelligence and security services are increasingly engaged in international cooperation. Through this they share increasing quantities of information across national borders, including sensitive personal data. This development brings new challenges for oversight bodies as well. Therefore, the Committee cooperates with foreign oversight colleagues at an unclassified level, in order to share experiences and improve oversight. Examples include discussions on oversight methods, the rulings of the European Court of Human Rights (ECtHR), staff training, the oversight of advanced technological systems and the oversight of bulk collection.

3.6.11. Conclusion

Since its establishment in 1996, the EOS Committee has overseen the intelligence and security services in Norway. A good dialogue with the services, as well as the presence of Committee members during inspections have been key elements in building the Committee's competence. They have built up a high level of mutual trust and respect with the services.

It is the Committee's opinion that strict regulation and oversight of the intelligence and security services is essential. Without a strong regulatory framework and consistent oversight, a situation could develop where national security concerns take precedence over other concerns in the day-to-day activities of the services. This would be to the detriment of privacy, democracy, and the protection of human rights. Regulatory developments in the last years have further clarified the legal basis for the services' activities. In newer legislation the services' authority to implement measures towards Norwegian citizens has been described in more detail. Consequently, the Committee's remit for oversight has also become more specific and detailed.

The Committee has contributed to increased awareness of rule-of-law considerations in the services. The preventive effect of the oversight – through the presence of the Committee and questions members ask – is of great importance. Key factors in maintaining this effect are the Committee's independence from both the government and the Storting, the fact that it oversees all the intelligence and security services, and its wide access to information. It is also worth mentioning

the importance of granting the Committee sufficient budgets and resources, which the Storting does. It is also essential to ensure that both the Committee and the Secretariat comply with their strict duty of secrecy, both to avoid harming national security and to build trust with the services.

Permanent oversight procedures increase the services' focus on compliance and their legitimacy in an open democratic society. It will always be a challenge to balance the need for national security and the right to individual freedom and privacy. This must be done both in legislation and in the daily activities of the services. It is the Committee's duty to take a critical approach to the services' actions, while the services must be able to use the freedom of action that the legal framework provides. Both the intelligence and security services and the EOS Committee will continue to work to uphold this balance in Norway.

3.7. Ukrainian case study: Democratic civilian control over the activities of the Security Service of Ukraine

Daryna Yarytenko and Denys Zaskoka

The Security Service of Ukraine is a special-purpose state body with law enforcement functions that ensures the national security of Ukraine.

Since the beginning of the anti-terrorist operation in April 2014, the nature of threats to Ukraine's national security has changed, which has also affected the nature of the deployment of the forces and resources of the Security Service of Ukraine. While in 2014 the threats were viewed as hybrid aggression with local combat zones, Russia's full-scale invasion in 2022 posed a much greater threat.

Influenced by the development of technologies, methods and techniques used by the enemy to carry out reconnaissance, sabotage and terrorist activities, the main priority for the SSU has become the quick adjustment of its activities to counter such threats, moving away from the classic model of a special service—solely gathering intelligence and counterintelligence information.

Since the beginning of the full-scale invasion in 2022, the most effective model for the SSU has been a combination of combat operations, counterintelligence, and investigation of crimes against Ukraine's national security. The SSU's activities have focused on the following areas: counterintelligence; counterterrorism; cybersecurity; protection of state secrets; and the detection, prevention and investigation of criminal offences in these areas.

At the same time, the SSU was stripped of non-core functions, in particular in: corruption prevention; organised crime as a 'police' function; and the investigation of 'economic crimes'.

The jurisdiction of the SSU is comprehensive and clearly defined by law. In accordance with Article 216 of the Criminal Procedure Code of Ukraine, the Service is responsible for investigating: crimes against the foundations of national security; against peace, humanity and international law; terrorist crimes; and crimes relating to state secrets.[490]

490 Verkhovna Rada of Ukraine, 2012. '*Criminal Procedure Code of Ukraine, No. 4651-VI, 13 April.*' Available at: https://zakon.rada.gov.ua/laws/show/4651-17#Text. [Accessed 14 October 2025]

Counterintelligence is the foundation of national security. To be one step ahead of the enemy, Ukrainian special services are constantly improving their methods and techniques. They rely on experience and take into account the development of technologies and methodologies used by the enemy in its subversive activities. The SSU's counterintelligence service operates 24/7, although its work remains largely invisible to the public.

The SSU regularly detects and successfully thwarts Russian special services' attempts to destabilise the country. Thus, the key challenges and threats to Ukraine's state security remain the active actions of Russian special services aimed primarily at: overthrowing the constitutional order or state power; reducing defence and economic potential; internal destabilisation; pushing society to surrender to the Russian federation; undermining all components of our state's resilience in repelling the aggressor; as well as undermining the trust of Ukraine's international partners.

Examples of the SSU's effectiveness include:

- The unprecedented special operation 'Pavutyna' (Spider Web), when SSU drones simultaneously wiped out one-third of Russia's strategic aviation: 41 aircraft were destroyed at key Russian airbases, as well as joint operations with military intelligence, which resulted in Russia losing its dominance in the Black Sea (combining combat, intelligence and counterintelligence components). All operations were carried out in accordance with international humanitarian law.

- The exposure of 113 enemy agent networks since the beginning of the full-scale invasion, which included more than 500 people. Their tasks were: agent and technical reconnaissance; sabotage and terrorist attacks; and information and propaganda activities.

The effectiveness of the fight against internal enemies directly depends on public trust in the special services, and transparent and properly established civilian control shows that the SSU's activities are open and predictable, thereby eliminating doubts about the lawful nature of its actions. Maintaining this balance strengthens the internal stability of the state, increases the effectiveness of countering hybrid threats, and confirms that even during wartime, Ukraine acts according to the rules of a law-abiding and democratic state.

Thus, democratic civilian control over the activities of special services, in particular the Security Service of Ukraine, is a key element for a democratic state governed by the rule of law. Its task is to ensure the accountability and transparency of the actions of security agencies, prevent abuse of power and guarantee respect for human rights and freedoms. In the context of modern hybrid threats, in particular martial law, ensuring the effectiveness and legality of the activities of special services is vital, which is only possible with a developed system of supervision by the state and society.

The legal framework for democratic civilian control is provided by: the Constitution of Ukraine; the Law of Ukraine 'On National Security of Ukraine'; the Law of Ukraine 'On the Security Service of Ukraine'; as well as other acts regulating the activities of parliamentary committees; the right to access public information; the activities of the Ukrainian Parliament Commissioner for Human Rights; and financial and anti-corruption control institutions.[491] The Comprehensive Strategic Plan for Reforming Law Enforcement Agencies as Part of the Security and Defence Sector for 2023–2027 (approved by Decree of the President of Ukraine No. 273 of 11 May 2023) and the Roadmap on the Rule of Law (prepared as part of Ukraine's commitments provided for in the European Union's Negotiating Framework, approved by the Decision of the Council of the European Union of 21 June 2024, under Cluster 1 'Foundations of the EU Accession Process'; approved by the Cabinet of Ministers of Ukraine on 14 May 2025 No. 475-r) provide for the extension of democratic civil control, including civil society.

The system of democratic civilian supervision over the activities of the SSU has a multi-level structure and includes several interrelated mechanisms: parliamentary; presidential; judicial; financial; anti-corruption control; public and prosecutorial oversight; as well as state registration of normative and legal acts.

The central institutional element of the democratic civilian control system is parliamentary control, which is exercised through the Verkhovna Rada (Ukrainian parliament). The parliamentary control system covers both permanent control measures and *ad hoc* measures. In particular, permanent areas of work include: hearing reports from the heads of special services; conducting parliamentary hearings; obtaining information in response to parliamentary questions/appeals; and analysing the results of the activities of special services in terms of their compliance with the Constitution and laws of Ukraine.

Ad hoc measures include meetings of the parliamentary committee on relevant issues, work of a temporary investigative commission or a temporary special commission of the Verkhovna Rada of Ukraine, etc.

The Head of the Security Service of Ukraine submits a written report on the activities of the SSU, including those carried out during the legal regime of martial law, to the parliament by 1 February each year. The Verkhovna Rada Committee on National Security, Defence and Intelligence (hereinafter referred to as the National Security Committee) plays a key role in this process. It performs control functions on behalf of the Verkhovna Rada of Ukraine in accordance with the Constitution of Ukraine over the activities of the special services. It also considers at its hearings issues related to the state of preparedness and response to real and potential threats to the national security of Ukraine. It reports on the activities

491 Verkhovna Rada of Ukraine, 1996. 'Constitution of Ukraine, No. 254к/96-ВР, 28 June.' Available at: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text; Law of Ukraine, 1992. 'On the Security Service of Ukraine, No. 2229-XII, 25 March.' Available at: https://zakon.rada.gov.ua/laws/show/2229-12#Text. [Accessed 14 October 2025]

of the SSU, and prepares proposals for legislative regulation of activities, in particular of special services, and provides relevant recommendations to state bodies within its competences.

Currently, the Constitution and laws of Ukraine do not grant the National Security Committee broader powers in terms of exercising parliament's control functions compared to other parliamentary committees. In addition, members of the Rada, including members of the National Security Committee, are granted access to state secrets of all classification levels by virtue of their office after signing a written undertaking to preserve state secrets (Article 27 of the Law of Ukraine 'On State Secrets').

Since the introduction of martial law in Ukraine, the importance of parliamentary control exercised by the Committee on National Security has increased. The special services regularly and periodically inform this Committee about the state and nature of threats to national security and the results of the activities of the special services. Indeed, the Committee holds closed meetings with the leadership of the special services to discuss issues related to the security situation in Ukraine.

3.7.1. On the future Verkhovna Rada Committee on control over Special Services

A special place in the system of democratic civilian control will be given to the specialised Committee of the Verkhovna Rada on Control over the Activities of Special Services after its establishment. The legislative regulation of its powers is stipulated in Article 33-2 of the Law of Ukraine 'On Committees of the Verkhovna Rada of Ukraine', which was added pursuant to the adoption of the Law of Ukraine 'On Intelligence' in September 2020.[492]

It should be noted that Article 33-2 of the aforementioned Law is not yet in force, as the Committee itself has not been established: it will come into force after the election of the new Verkhovna Rada of Ukraine and its decision on the appointment of the relevant committee's members. However, in accordance with the Constitution of Ukraine, elections of People's Deputies may be held after the end of martial law.

The members of the Committee will be elected by the Verkhovna Rada in accordance with the procedure applicable to all parliamentary committees: membership will be formed by a decision of the parliament on the basis of proposals from parliamentary groupings in compliance with the quotas established by the regulations of the Verkhovna Rada. Their term of office will effectively

492 Law of Ukraine, 1995. 'On Committees of the Verkhovna Rada of Ukraine, No. 116/95-BP, 4 April.' Available at: https://zakon.rada.gov.ua/laws/show/116/95-%E2%F0#Text Accessed 14 October 2025].

correspond to the current parliament's mandate, but the composition may be adjusted at any time by decision of the Verkhovna Rada.

Regarding professional expertise and additional criteria, the Law of Ukraine 'On Committees of the Verkhovna Rada of Ukraine' does not establish any special requirements for work experience. All members of the Committee must be current members of parliament. However, Part 4 of Article 33-2 of this Law stipulates that the requirements to be met by a member of the Committee and an employee of the Committee Secretariat must be determined by the Verkhovna Rada. In other words, the Rada still has to determine the relevant requirements.

At the same time, the legislation grants future members of the special parliamentary committee broader rights than other members of the Ukrainian parliament (in particular, the right to freely visit special services institutions, access sensitive information, etc.). However, they will only be able to exercise these rights after undergoing a comprehensive security procedure: special inspection, verification and obtaining clearance and access to state secrets, and access to intelligence secrets in accordance with the procedure established by law.

The procedure for organising and conducting special inspections, the frequency of such inspections and the appeal procedure against said results will be approved by the Verkhovna Rada itself in a separate act (Part 4 of Article 33-2 of the Law of Ukraine 'On Committees of the Verkhovna Rada of Ukraine'). Within the same procedure, a security clearance will be carried out by the Security Service of Ukraine as the authorised state body in state security in accordance with the Law of Ukraine 'On State Secrets'. In the event of a negative conclusion, the People's Deputy of Ukraine will be able to appeal to the Committee on the Organisation of the Verkhovna Rada's Work, Regulations and Deputy Ethics regarding the special inspection; or to the court regarding the security clearance in connection with access to state secrets.

The Committee will, in particular, be authorised to submit written recommendations for consideration, initiate inspections or official investigations in case of doubts regarding the legality of the actions of the special services. In addition, it will be possible to hear the heads of the services at closed meetings, which will allow MPs to obtain sensitive information within the framework of confidential access.

If violations are detected, the Committee will have the power to initiate disciplinary proceedings or to propose the temporary suspension of officials while investigations are ongoing. Such measures are aimed at ensuring a rapid response to abuses of power and at establishing legal accountability in the security sector. This will enable the Committee to exercise control not in a declarative manner, but with due regard for all the specific features of the activities of the special services.

A separate area of parliamentary control is the prevention of abuse of power by the special services. Response mechanisms include both the initiation of official inspections and the conduct of disciplinary investigations into individual officials.

The Committee will be able to raise issues regarding the illegal conduct of covert operations, abuse of power during arrests, the use of special services for political purposes, or illegal interference in the activities of public authorities. Based on the results of inspections, not only temporary dismissal from office is possible, but also the opening of criminal proceedings by the State Bureau of Investigations if signs of a criminal offence are found.

Monitoring human rights is a separate part of what Parliament is responsible for. In this context, the Ukrainian Parliament Commissioner for Human Rights plays an important role. He or she has the power: to investigate complaints from citizens about violations of their rights and freedoms by the special services; to monitor the living conditions of persons under arrest and the observance of their rights; and to inform the Ukrainian parliament about any violations found. The Ukrainian Parliament Commissioner for Human Rights also submits an annual report on the state of observance and protection of human and civil rights and freedoms in Ukraine.

As a result, parliamentary control over the activities of the special services in Ukraine is not just part of the legislative work. It is also a key element of democratic governance. It performs a restraining function in relation to the executive branch, ensures a balance between security and human rights and promotes greater public trust in state institutions. The effective functioning of the relevant parliamentary committee, the existence of a legal mechanism for access to restricted information and the procedural capacity to respond to violations are effective even under the difficult conditions of martial law.

The President of Ukraine, as the guarantor of the Constitution and Supreme Commander-in-Chief, plays an important role in the system for monitoring the activities of the security and defence sector, including the Security Service of Ukraine. The constitutional and legal mandate of the President in this area is set out in Articles 106 and 107 of the Constitution of Ukraine, as well as in Article 5 of the Law of Ukraine 'On National Security of Ukraine' and the Law of Ukraine 'On the Security Service of Ukraine'.[493] Control is exercised both directly and through a number of accountable and advisory institutions, in particular the National Security and Defence Council of Ukraine (NSDC), which coordinates the activities of all bodies in the security and defence sector.

One of the key instruments for ensuring the accountability of special services to the President is the obligation of the Security Service of Ukraine to regularly inform the Head of State. Pursuant to Part 3 of Article 32 of the Law of Ukraine 'On the Security Service of Ukraine', the SSU is required to systematically provide the President, members of the NSDC, and officials specially appointed by the President

493 Law of Ukraine, 2018. 'On National Security of Ukraine, No. 2469-VIII, 21 June.' Available at: https://zakon.rada.gov.ua/laws/show/2469-19#Text; [Accessed 14 October 2025]. Law of Ukraine, 1992. 'On the Security Service of Ukraine.'

with information on the main issues of its activities, including instances of legal violations. In addition, the Head of State has the right to request other information needed to carry out control functions.

Part 4 of the same article establishes the obligation of the Head of the Security Service to submit an annual written report on the SSU's activities to the President. This is not only an official mechanism for providing information, but also a basis for assessing the effectiveness and legality of the Service's activities from a strategic perspective.

The National Security and Defence Council of Ukraine plays a key role in coordinating control over the activities of the entire security sector. In accordance with Article 107 of the Constitution of Ukraine and the provisions of the Law of Ukraine 'On the National Security and Defence Council of Ukraine,' the NSDC is the main interdepartmental body for planning, coordinating and monitoring the implementation of national security policy.[494] The NSDC considers issues related to the operation of special services, approves strategic planning documents, and formulates key directions of state policy in the field of security.

The integrity of this model of presidential control is enhanced by the possibility of creating special consultative, advisory and other auxiliary bodies and services under the President of Ukraine, which may be engaged in the exercise of his control functions as required. An example of such a body is the coordinating body on intelligence issues – the Intelligence Committee, established by the President of Ukraine in 2020. The main task of this Committee is to prepare proposals for the President of Ukraine on the management, coordination and control of the activities of the state intelligence agencies. Its members are appointed by presidential decrees on the recommendation of the Committee chair, who is currently the head of the Main Intelligence Directorate of the Ministry of Defence of Ukraine. Sessions are held on an *ad hoc* basis, mainly to discuss coordination of joint activities by intelligence community entities to counter threats to national security.

Such institutional flexibility allows for strategic and tactical control in the field of intelligence, counterintelligence and security in general.

Judicial control is one of the fundamental elements of democratic civilian control over the activities of intelligence services, which ensures the observance of human rights and freedoms in the exercises of security bodies. It serves as a legal safeguard against abuse and unjustified restriction of citizens' rights by the security forces. It is a key democratic instrument that ensures that the activities of security agencies comply with constitutional guarantees of human rights and international standards. Thus, judicial control forms one of the most important stages in the multi-level system of democratic civilian control.

494 Law of Ukraine, 1998. 'On the National Security and Defense Council of Ukraine, No. 183/98-BP, 5 March.' Available at: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text. [Accessed 14 October 2025]

The legal framework for judicial control is defined by the Constitution of Ukraine, the Criminal Procedure Code, the Law of Ukraine 'On Operational and Investigative Activities' and the Law of Ukraine 'On Counterintelligence Activities'.[495] According to these regulations, any actions related to interference with an individual's private life may only be carried out by a court decision. This applies, in particular, to covert entry into a person's home or other property, interception of information from communication channels, control of correspondence, telephone conversations, communications, and the use of special technical means to collect information.

Within criminal proceedings, judicial control is exercised by an investigating judge who is authorised to consider motions of the prosecution (prosecutor, investigator, detective) regarding procedure permits. This includes permits for searches, arrests, detentions, covert investigative (detective) actions and other procedural actions that may affect an individual's rights. In addition, the observance of the rights of detainees is monitored at this stage. Thus, the judiciary acts not only as an arbitrator in legal disputes, but also as an active guarantor of the rights and freedoms of individuals under control or suspicion of the special services.

A separate area of judicial control is the consideration of complaints against the actions or inaction of SSU personnel. Individuals who believe their rights have been violated as a result of the actions of the special services are able to appeal to the courts.

Particular attention should be paid to maintaining a balance between the need to ensure state security and the protection of human rights. In this context, effective judicial control should be based on the independence of the judiciary, transparency of procedures for approving covert measures, and the availability of specialised judges with the requisite training and access to classified information.

The proper balance between the needs of counterintelligence and human rights is ensured by a strict procedure for granting court permission for certain counterintelligence activities. This is set out in Article 8 of the Law of Ukraine 'On Counterintelligence Activities' and Chapter 21 of the Criminal Procedure Code of Ukraine. Any interference by the SSU that restricts constitutional rights (wiretapping, interception of information from communication channels, covert search of a home, etc.) may be carried out only upon a reasoned ruling by an investigating judge of the court of appeal. The term of such a ruling is no more than two months, after which a new application with updated proportionality justification is required. The applications are automatically distributed among investigating judges who already have access to state secrets.

Prosecutorial oversight is one of the components of the system of democratic civilian control over the activities of special services in Ukraine.

495 Law of Ukraine, 1998. 'On the National Security and Defense Council of Ukraine.'

In Ukraine, the functions of the prosecutor's office are defined in Article 131-1 of the Constitution of Ukraine. Its functions include conducting public prosecutions in court, providing procedural guidance of pre-trial investigation, addressing other matters in criminal proceedings as provided by law, overseeing covert and other investigative and detective activities of law enforcement agencies, and representing the state in court.

3.7.2. Oversight in criminal proceedings

In criminal proceedings, prosecutorial oversight ensures compliance with the law during pre-trial investigations, in particular in cases under the jurisdiction of the Security Service of Ukraine. In accordance with the Criminal Procedure Code of Ukraine, the prosecutor oversees the investigation, issues notifications of suspicion, approves indictments, and conducts public prosecution in court.

In addition, the prosecutor is empowered: to assess the legality of the actions of SSU investigators; to annul unlawful or unfounded decisions; to request additional investigative actions; and to submit appropriate motions to the court to ensure the rights of suspects, victims and other parties involved in the proceedings.[496]

Prosecutorial oversight is of particular importance in measures related to the temporary restriction of human rights, such as detention, arrest, search or covert investigative measures. In these cases, the prosecutor serves as a guarantor of the legal order and balance between the needs of the investigation and the constitutional rights of the individual.

3.7.3. Oversight of counterintelligence activities

The Constitution of Ukraine and the Law of Ukraine 'On the Public Prosecutor's Office' do not provide the public prosecutor's office with the function of oversight of counterintelligence activities in general, and the provisions of Part 3 of Article 2 of the Law of Ukraine 'On the Public Prosecutor's Office' explicitly prohibit vesting the public prosecutor's office with powers not provided for by the Constitution of Ukraine.

At the same time, Article 7 of the Law of Ukraine 'On Counterintelligence Activities' provides that measures related to the temporary restriction of human rights are carried out only by a ruling of an investigating judge. The ruling is issued upon the request of the head of the relevant operational unit, approved by the Prosecutor General or their deputy.

496 Law of Ukraine, 2014. 'On the Prosecutor's Office, No. 1697-VII, 14 October.' Available at: https://zakon.rada.gov.ua/laws/show/1697-18#Text. [Accessed 14 October 2025]

Thus, the Constitution of Ukraine and the Law of Ukraine 'On Counterintelligence Activities' provide for the oversight function of the prosecutor's office solely in relation to measures that temporarily restrict human rights.

3.7.4. Oversight of operational and investigative activities

According to Article 14 of the Law of Ukraine 'On Operational and Investigative Activities', prosecutorial oversight of operational and investigative measures is exercised by the Prosecutor General, their deputies, the heads and deputy heads of regional prosecutors' offices, as well as authorised prosecutors of the Office of the Prosecutor General. This framework establishes a vertically integrated system of oversight, with a clearly delineated set of officials responsible at each level of prosecutorial hierarchy.[497]

In practical terms, prosecutorial oversight encompasses oversight of the legality of decisions, actions or omissions by officers of the SSU in the course of their operational and investigative functions. The prosecutor has the right to annul unlawful or unjustified decisions, initiate disciplinary or criminal proceedings in case of violations, and require the cessation of any illegal actions. Particular emphasis is placed on overseeing the observance of detainees' rights and ensuring the proper execution of court decisions involving the temporary restriction of personal liberty.

The detained person receives a set of procedural guarantees provided for by law, which are under constant prosecutorial oversight. Immediately after the actual detention, the investigator or SSU operative is obliged to explain to the detainee in understandable language: the grounds for detention; the reasons for suspicion; the right to remain silent; the right to notify relatives; and the right to a lawyer.

According to the Criminal Procedure Code, access to a defence lawyer is guaranteed from the moment of actual detention. The investigator, prosecutor and court must: facilitate contact, ensure confidential meetings without time or number restrictions; and provide the opportunity to use communication means to invite a lawyer.

The Constitution of Ukraine requires that the validity of detention be reviewed within 72 hours; if a court order is not delivered, the person must be released. A request by the prosecutor (or investigator, with the prosecutor's consent) for a preventive measure must be considered immediately, but no later than 72 hours from the moment of actual detention. The investigating judge's ruling is valid for no longer than 60 days and can be extended only by a substantiated new decision.

497 Law of Ukraine, 1992. 'On Operational and Investigative Activities, No. 2135-XII, 18 February.' Available at: https://zakon.rada.gov.ua/laws/show/2135-12#Text. [Accessed 14 October 2025]

This mechanism is a vital component of the broader architecture of democratic civilian control. It allows for independent legal monitoring of the actions of the special services at every stage, from suspicion of a person of committing a crime to the final court decision. In addition, the prosecutor's office has the potential to prevent systemic human rights violations by identifying and eliminating legal gaps in the procedures employed by law enforcement agencies.

In a democratic state, **civil society** is not merely a recipient of state policy, but also an active subject of its formation and control. Given the specifics of the activities of special services, public engagement in their oversight is of particular significance, as it introduces an additional layer of transparency, enhances institutional accountability, and fosters public trust in the security sector. Even under martial law, civilian oversight mechanisms remain an essential element of democratic governance. They ensure that the activities of the special services remain within the bounds of legality and that secrecy is driven solely by national security concerns, rather than being employed as a means of avoiding public accountability.

In Ukraine, these functions are carried out through a range of public oversight instruments, established both under general access-to-information legislation and *via* institutional mechanisms that facilitate interaction between civil society and public authorities.

The main areas of public oversight are: monitoring by non-governmental organisations and journalists; submission of appeals to the Ukrainian Parliament Commissioner for Human Rights in cases of violation of citizens' rights; as well as public discussion of the activities of the special services in the media, through analytical reports, thematic publications and interviews.

In this context, it is important to note the disclosure of classified information. Criminal liability for disclosing state secrets (Article 328 of the Criminal Code of Ukraine) applies primarily to officials who are the bearers of classified information; a journalist who publishes correspondence or documents that have already been leaked to him or her usually appears as a witness in the case or is not prosecuted at all. The most high-profile example is the search of the Strana.ua editorial office in 2017 on suspicion of publishing secret files of the Ministry of Defence of Ukraine: the journalists were not taken into custody, instead the investigation focused on the sources of the leak. There have been no cases of actual imprisonment of Ukrainian journalists for materials relating to the special services.

Polygraph tests can be used as an additional tool. The results of polygraph tests do not have the procedural force of evidence in court, but they do allow investigators to narrow down the circle of potentially involved persons in an internal investigation. Thus, the system is designed to punish those guilty of leaking classified information, rather than journalists.

The Law of Ukraine 'On National Security of Ukraine' also provides for the mandatory periodic publication of analytical documents such as 'White Papers', national reports, and sectoral reviews. This not only increases the transparency of the security sector but also contributes to a better understanding of the tasks and challenges faced by the special services.

Restrictions on public oversight may be imposed solely in the interests of protecting classified information.

The legal framework guarantees registered civic associations the right to access information from public authorities, including those within the security and defence sector, except for data classified as being restricted. These kinds of associations are: entitled to conduct research on national security matters; present their findings; participate in public discussions; initiate public examination of draft legal acts; and submit their conclusions for official consideration. This forms an open political ecosystem in which civil society can meaningfully influence state security policy at an expert level.

The institutional mechanism for informing the public holds a special place within the framework of interaction between the civil society and security agencies. Under Article 7 of the Law of Ukraine 'On the Security Service of Ukraine', the SSU keeps the public informed about its activities through the media, responds to inquiries, and uses other forms provided for by law. In particular, by publishing periodic public reports ('White Papers') that inform the public about the SSU's mission, values and principles, outline the directions of the SSU's transformation, highlight the priorities and main results of the SSU's activities and ensure transparency of the SSU's work.

In peacetime, and even more so during martial law, the duty of security agencies to keep the public informed takes on particular significance. The Security Service of Ukraine regularly updates the public on: the detection and investigation of crimes against the foundations of national security; measures to counter intelligence and subversive activities; prevention of terrorist acts; ensuring the information security of the state; and the documentation of the aggressor's war crimes. This information is posted on the SSU's official website, in particular in the form of activity reports and press releases, in verified social media channels and in media reports.[498] The SSU's digital platforms currently rank among the most widely accessed of all Ukrainian security and defence agencies.

The SSU also responds to requests from media representatives, assists in the preparation of journalistic materials, and addresses to citizens' appeals for the protection of their rights, including in relation to investigations of specific criminal

498 Security Service of Ukraine, n.d. 'Democratic Civilian Control'. Available at: https://ssu.gov.ua/en/demokratychnyi-kontrol. [Accessed 4 November 2025]

proceedings. Information on the processing of requests for information received by the SSU is available on the SSU's official website. Thus, the information function becomes a two-way communication process, thereby enhancing the SSU's openness to the public.

Financial transparency and the prevention of corruption are essential components of effective democratic civilian control of the activities of intelligence services. Given that the work of agencies such as the Security Service of Ukraine often involves the use of funds subject to restricted access, including covert expenditure, it is vital that their spending is subject to systematic and independent audit. In democratic systems, financial and anti-corruption control serves to uphold the rule of law and bolster public trust in security services.

The financial transparency of the Security Service of Ukraine is limited by the legislation on state secrets and is therefore implemented mainly in the form of aggregate indicators. There are no separate 'special expenditures' in the public domain, as their details are directly classified by law as restricted information. The SSU publishes its financial statements on its official website.

In Ukraine, several institutions control the budgetary use of SSU resources. The Accounting Chamber, in accordance with Article 1 of the Law of Ukraine 'On the Accounting Chamber', exercises, on behalf of the Verkhovna Rada of Ukraine, authority over the receipt and utilization of state budget funds. This encompasses both general funding and expenditures allocated to the security and defence sector. The Accounting Chamber conducts audits, prepares assessments of the effectiveness of fund utilization, and reports to the Parliament. Its activities provide an independent external evaluation of the financial discipline within the special services.

The Ukrainian Ministry of Finance, as a central executive body, is responsible for implementing state policy in the field of financial control, including the analysis of the use of classified expenditures. This activity is carried out within the constraints established by the Law of Ukraine 'On State Secrets', yet it ensures the fiscal accountability of executive bodies, even in sensitive areas.[499]

The anti-corruption aspect of control is ensured by the activities of the National Agency for the Prevention of Corruption (NAPC). According to Part 7 of Article 19 of the Law of Ukraine 'On the Security Service of Ukraine', all SSU employees required to declare assets must submit a declaration of a person authorised to perform the functions of the state or local self-government by 1 April each year. This obligation is regulated by the provisions of the Law of Ukraine 'On Prevention of Corruption' and applies to a wide range of officials, including those with access

499 Law of Ukraine, 1994. 'On State Secrets, No. 3855-XII, 21 January.' Available at: https://zakon.rada.gov.ua/laws/show/3855-12#Text. [Accessed 14 October 2025]

to particularly sensitive information. The NAPC verifies declarations for accuracy, identifies potential conflicts of interest and assesses the risks of misconduct.[500]

Together, these mechanisms form a multi-tiered system of financial control within the security sector, striking a balance between safeguarding national interests and upholding principles of transparency. Ensuring the lawful and efficient use of budgetary resources not only enhances the state's security capabilities but also reinforces its adherence to democratic standards of governance.

The Ministry of Justice of Ukraine contributes to ensuring democratic civilian control over the activities of security and law enforcement agencies by conducting legal expertise for regulatory acts. The main tasks of the Ministry of Justice include analysing draft legal acts for compliance with the Constitution of Ukraine, existing national laws, Ukraine's international obligations, and the case law of the European Court of Human Rights.

The Ministry of Justice's expertise is aimed at preventing the adoption of regulatory measures that might contravene human rights standards or undermine the rule of law. This approach ensures that regulations governing the activities of special services align with international norms on rights and freedoms protection and incorporate the practices of international judicial bodies, thereby safeguarding legal conformity.

In the national legal framework of Ukraine, torture is absolutely prohibited by the Constitution of Ukraine, international treaties of Ukraine, and laws of Ukraine, and cannot be a method of counterintelligence or counterterrorism under any circumstances. Indeed, its use is subject to criminal liability. In addition, in 2021, the Cabinet of Ministers approved the Strategy for Combating Torture in the Criminal Justice System, which provides for mandatory video recording of all investigative actions with detainees, enhanced prosecutorial oversight, the National Preventive Mechanism (Ombudsman's Office) and training modules for operational and investigative officers on ECHR standards.

Thus, the Ministry of Justice plays an important role within the democratic civilian control framework, ensuring that the legal regulation of the security sector meets both national and international legal requirements.

500 Law of Ukraine, 2014. 'On Prevention of Corruption, No. 1700-VII, 14 October.' Available at: https://zakon.rada.gov.ua/laws/show/1700-18#Text. [Accessed 14 October 2025]

3.7.5. Conclusion

The system of democratic civilian control over the activities of the Security Service of Ukraine is structured as a multi-tiered and functionally balanced framework that covers all the key areas: parliamentary, presidential, judicial, prosecutorial, financial, anti-corruption, and civic. Each of these mechanisms is firmly rooted in specific legal provisions, endowed with clearly defined powers and procedural tools for implementation, thereby ensuring both horizontal and vertical accountability of the SSU.

This system's primary purpose extends beyond merely guaranteeing the effective functioning of the special services. It is equally dedicated to establishing strong safeguards to prevent abuse of power, violation of citizens' rights, and to combat corruption.

To this end, national legislation provides a robust institutional and legal foundation designed to effectively deter misconduct, ensure transparency, and uphold human rights standards. Collectively, the system already covers the political and legal, organisational and information aspects of control, and its components operate in a coherent and coordinated manner within a unified framework, eliminating the need for any additional or parallel structures.

3.8. UK case study: Assessing and overseeing intelligence and law enforcement in the Euro-Atlantic area

David Watson

3.8.1. Overview

Like many of their Euro-Atlantic counterparts, the UK Security Service (MI5) does not have law enforcement functions. This is the same for the Intelligence Service (MI6) and the signals intercept agency (GCHQ). This is sometimes described as 'pre-trial investigation', although this term is confusing as it depends where you draw the line as to when pre-trial investigation actually begins. If a security agency hands a case to a Law Enforcement Agency (LEA) for possible prosecution, then considerable investigation has already taken place even if none of the investigation is ultimately used as evidence in a trial.

The view in the UK is that Security/intelligence agencies (SIA) have a different mandate from LEAs and that the roles should be separated. This is not because of possible human rights breaches. The UK view is that separation of powers to ensure there are sufficient checks and balances (especially where the SIA will have considerably greater investigatory powers), better accountability, operational secrecy, avoidance of the duplication of tasks and better use of resources (especially with regard to specialist training).

Most importantly, it separates the work of the SIA from prosecutions. This air gap allows all cases to be dealt with in the same way as any other criminal trial and it ensures prosecutions are made on the same criteria as any other criminal prosecution and that evidence is not hidden or the system manipulated in order to secure a conviction.

In the UK, the responsibility for arrest, detention, questioning and prosecution rests with the LEA and the judiciary. The agencies can work with any UK LEA and not just the police in order to pursue an operational case.

It would be very misleading to suggest that SIA investigates cases within its remit (in particular espionage and terrorism) and then at some point hands over the investigation wholesale to an LEA without further input or involvement. The relationship between the SIA and the UK LEAs is very close. Often, they will work alongside one another and even second staff into each other's teams to provide advice and continuity to investigations. This is especially the case with terrorism.

3.8.2. The law

The SIA mandate is primarily enshrined in two UK laws: the Security Service Act 1989 and the Intelligence Services Act 1994. Neither Act gives the SIA any law enforcement functions. Nor does either act proscribe the terms of any relationships with LEAs. Subsequent legislation such as Regulation of Investigatory Powers Act (RIPA), the Investigatory Powers Act (IPA) and the National Security Act (NSA) have further defined responsibilities and extended oversight mechanisms. In addition, other acts that define human rights, prosecution of terrorism and espionage have affected the work of the SIAs and their relationship with LEAs.

This makes the legal landscape and the relationship with LEAs complex and it requires professional legal advice. This is why all of the SIAs have teams of legal advisors to help the services and to offer advice on navigating the law relating to their work and in particular operations, as well as their relations with LEAs.

The key point in the relationship between the SIA and LEAs (other than who is responsible for bringing a case to trial) is *not* proscribed by law. This is important as it allows both the SIAs and LEAs to consider each case on its individual merits and ask how best to cooperate on a case-by-case basis.

3.8.3. Evolution of the relationship

The relationship between the SIAs and LEAs has evolved considerably over the last 30 years and especially since the SIA acts were put in place. Before this time, the SIA (primarily MI5) would investigate cases within its remit. When there was a *prima facie* case (i.e. a clear case) for possible prosecution, they would call in specialist police officers from a specialist vetted unit within the Police Service to consider and pursue prosecutions where necessary.

These 'Special Branches' would effectively review the case but would be required to build up a prosecution case based almost entirely upon evidence that they themselves were required to collect. It was highly unlikely that evidence from the SIA would be used in the prosecution. This would protect SIA techniques and would ensure that there was objectivity with regard to evidence used. However, this stark separation came under scrutiny due to increased terrorism in the UK and the need to act quickly to forestall any terrorist acts that put the public in danger. The system had been designed with espionage in mind rather than terrorism, which now needed much quicker response times.

3.8.4. The current situation

The situation in the UK is today very different. The SIAs work in partnership with LEAs and in the case of counter terrorism, the SIAs often work embedded in police teams. For example, the Counter Terrorism Operations Centre in London houses both the SIAs terrorism HQ alongside the Police terrorism HQ. This means that they work alongside each other during all stages of counter terrorism investigations and not just when the SIA believes there is a *prima facie* case for prosecution. By doing this, it means that all information can be exchanged and shared, as well as ensuring the efficiency of any operation.

It is still the responsibility of a LEA to lead on gathering evidence that would be put before a trial. The ultimate decision to prosecute rests neither with the LEA nor the SIA but with the Crown Prosecution Service (CPS). The CPS in the UK prosecutes criminal cases that have been investigated by the LEAs. The CPS is an independent body which makes the decision to prosecute completely independently of the police or government. In addition to deciding which cases should be prosecuted, it determines what specific charges should be made, will advise the police during the early stages of an investigation, prepares cases and presents them at court and provides support to victims and witnesses. This ensures the absolute independence of the prosecution process.

SIA intelligence may be admitted in evidence and disclosed to the defence. But this is largely in relation to terrorism and there is still a desire for LEA to independently gather its own evidence for prosecution. Some SIA officers have given evidence, but it is up to the individual judge to see whether this can be done anonymously or in public. Either way, the officer is subject to cross examination in the normal way. This reinforces the view that independent evidence gathered by LEAs is preferable and also ensures that evidence is strong rather than relying on a single strand of information.

Even intelligence that is not relied on by the prosecution in evidence but that is potentially relevant to the case, needs to be reviewed by prosecutors. If it is deemed to be 'reasonably capable' of undermining the prosecution or aiding the defence, then it must be disclosed. This means that potentially all information must be made available. Sometimes, this can lead to cases being dropped as the disclosure of information would have a serious effect on national security. In certain cases, if it is believed that the disclosure of the intelligence could undermine national security, then a relevant government minister can apply for a Public Interest Immunity (PII) to stop disclosure. However, PIIs are rarely used. In addition, it is up to trial judge to either accept or deny the request.

3.8.5. Case example

Operation Crevice was a 2004 joint SIA/Police operation which led to the prosecution of six terrorists who were planning to construct a bomb that was potentially going to be used against a shopping centre. The source of the intelligence that led to the investigation and subsequent arrests was said to be an intercept of Al-Qaeda leaders in Pakistan to militants in the UK. The subsequent operation to investigate the case was handed to anti-terrorist Police who were able to build a case and evidence against the accused. Bomb-making equipment was found in garages, and the individuals were prosecuted. So, whilst the initial investigation might have started with SIA intelligence, the subsequent gathering of evidence for the CPS was made by an LEA, namely the anti-terrorist Police.

3.8.6. Oversight

As SIAs in the UK do not have law enforcement powers, there are no specific oversight laws that refer to the LEA powers of SIAs. This is because the pre-trial investigation of matters such as espionage, serious crime and terrorism are conducted by the LEAs. Oversight of SIAs is through the following means:

- Parliamentary oversight through the Intelligence Services Committee (ISC) which deals with expenditure, administration, policy and operational activity (but only retrospectively). They do not have any involvement in the relationship between SIAs and LEAs as such. This is due to a separation between the UK government and the 'due process of law.' However, it is possible that the ISC might look at a case retrospectively from an operational standpoint.

- Judicial oversight through the Investigatory Powers Act (IPA), which deals with oversight of communications; and the Regulation of Investigatory Powers Act (RIPA), which deals with the covert surveillance of individuals with regard to their human rights. Neither act deals specifically with the role of SIAs in prosecutions.

- Executive oversight is conducted through the Prime Minister and any other relevant minister (either Home Affairs or Foreign Affairs). This oversight is centred around the tasking of the services and permissions for certain operations (usually associated with political risks).

- Internal oversight. Every service has its own set of rules and guidelines to ensure that staff act ethically, morally and within the law. Each member of staff is given legal and ethical training on a regular basis, especially if dealing with operational matters.

- As can be seen, most oversight is centred on operations and investigations within the remit of the SIA laws. They do not extend to relationships with LEAs.

However, the LEAs and CPS have their own oversight mechanisms which are many in number, but that again do not refer to the relationship with SIAs. This is because pre-trial investigation and prosecution are not part of the SIA remit. It is possible that there could be enquiries conducted into prosecutions and the gathering of pre-trial evidence, but they are most likely to be centred around the LEA pre-trial investigation and the decision of the CPS to prosecute. If there was faulty intelligence received from the SIA then the LEA and CPS should have made sufficient steps to ensure its veracity before proceeding further and any enquiry would more likely focus on the LEA and CPS role.

The specific laws governing prosecution in terrorism, espionage and serious crime do not refer to the SIA in any way. There is an independent reviewer of terrorism legislation whose role also looks at state threats. But the reviewer's role is solely to review legislation rather than prosecutions or investigations.

3.8.7. The courts

With regard to matters of espionage, terrorism and serious crime, the cases would be heard as a normal criminal case within the UK Crown Court system. There will be a judge who will run the court case and a jury of twelve adults who are randomly selected. There is specialist advice to judges on conducting terrorist trials (see Conduct of Terrorist trials by Sir Charles Hadden-Cave on www.judiciary.uk) but this is independent of SIA involvement. However, it is important to note that advice to trial judges is advisory and not mandatory. This is to ensure the independence of the judiciary.

It is up to the judge to decide what evidence is admissible. The accused has the right to be represented by a legal counsel. In rare cases, some evidence may be withheld from the defence under a public interest immunity request or through closed court sessions especially in such cases as the deportations of suspected terrorists. However, these are at the discretion of the trial judge.

SIA members can be called as witnesses in specific cases and may be able to give evidence to the court from behind a screen to protect their identity. Again, this is at the discretion of the trial judge.

In Northern Ireland, there are the 'Diplock' criminal courts. These are named after Lord Diplock who was tasked by the British government in 1972 with looking into a variety of issues relating to dealing with Irish Republican terrorism and suggested a way of dealing with potential intimidation of juries. In a Diplock court, the trial is conducted solely by a judge. These continue to this day, but special permission must be sought and these courts have nothing to do with SIA involvement.

3.8.8. Advantages and disadvantages of the UK system

When looking at the UK system and the relationship between SIAs and LEAs there are positive and a few negatives in this type of system as discussed below.

3.8.8.1. Advantages

- There is little doubt that SIAs in any country have wide ranging powers that by necessity involve intrusive surveillance of the population. Further to this, SIAs work directly with the government and could easily be encouraged to be working on cases that may have a political motive rather than being for the good of society. In the UK, there is the safeguard that by not being able to carry out pre-trial investigations or prosecutions, there is an effective air-gap between an SIA-led investigation and prosecution.

- Investigations carried out by SIAs are placed under double scrutiny if they are to be considered as possible prosecutions: first by the LEAs and then by the CPS. Evidence cannot be hidden from the defence and there has to be a clear *prima facie* case for prosecution. There is a reduced chance of relying on circumstantial evidence as scrutiny has taken place at all three stages (SIA, LEA and CPS) ensuring that evidence is fully scrutinized.

- The SIAs cannot carry out questioning of suspects and witnesses under this system. There is always the possibility of leading witnesses based on assumptions in any criminal case, but where there is a great deal of information, this can lead to biased judgments based on assumptions. Independent LEAs will be less prone to this weakness.

- One of the biggest advantages is that this system is stronger in protecting sources and techniques. When a LEA takes over the investigation, it can investigate the case separately and establish its own chain of evidence without compromising SIA sources. For example, if a SIA has a source overseas within a terrorist network, then the SIA can alert LEAs to a potential terrorist in the UK. The LEA can then gather independent evidence on the UK-based individual to see if he or she is a terrorist. If they are then the responsible LEA can use their own evidence without compromising the SIA overseas source.

- Only special units with UK LEAs will prosecute cases that are driven by SIAs. These units are vetted to the same standards as SIA staff so that discussions on cases and prosecutions can be completely open without further security considerations. The co-location of teams means that all aspects of cases can be discussed at any point during investigation and potential prosecution. This also means that the LEAs can act promptly if an SIA investigation uncovers an immediate danger to life or property.

- The close working between the SIA and LEAs builds trust and the ability to exchange techniques.

- The UK system is underpinned by internal oversights and rules within SIAs and LEAs. These oversights ensure that the law is upheld and not manipulated as well as having safeguards through oversight of each stage of the process of prosecution.

- The range of what SIAs can investigate (and may lead to possible prosecution) is strictly controlled by their mandate.

3.8.8.2. Disadvantages

- The most significant disadvantage is that SIAs can easily lose control of the operation once it is handed over to LEAs. The LEA may feel they have to act on a case, and this could compromise sources and techniques across a wide range of operations thus leading to loss of sources and revealing sensitive intelligence methods.

- It could be argued that due to the closeness of SIAs and some LEA units, it is actually the same as the SIAs having law enforcement powers. It could be argued that they are effectively a single entity, and the only air gap is when the case is handed to the CPS.

- The separation of law enforcement powers is rigid and does not allow flexibility in a rapidly changing world. Hybrid warfare is on the rise and both the SIA and LEAs need to respond quickly. For example, cyber-crime can easily be terrorist related or state sponsored and allowing SIAs to conduct pre-trial investigations may speed up prosecutions. There is also a risk of duplication of tasks and expertise in a world where both are limited. Social media can be used as a method to attack the state just as much as an act of espionage or terrorism, and it may be the state needs to be much more careful in protecting knowledge of its surveillance methods. Complete openness can damage the state's ability to protect itself.

- The separation makes the use of intelligence from overseas services (liaison) more difficult. There will be a need to protect this sensitive liaison information by the UK SIA services which might run against the desire by LEAs to pursue an open criminal case. It is often difficult to navigate between protecting the liaison source or technique and acting.

3.8.9. Conclusion

The separation of SIA investigations and intelligence gathering from pre-trial investigation is well established in the UK. The initial motivation for this was the need to protect sources and techniques and centred around law enforcement establishing their own pre-trial evidence following discussions with the SIAs. Whilst there have been some parts of UK society that have questioned SIA powers with regard to prosecutions, it has been almost universally accepted that the SIA works in the best interests of UK society. As a result, the oversight of the SIAs and their relations with law enforcement have been relatively light. Virtually all prosecutions resulting from SIA investigations have been dealt with entirely within the open criminal justice system and not separated out into secret courts or other restrictive practices.

This very clear separation has come under strain with increased terrorism and the rise of state-sponsored hybrid warfare. It is no longer feasible in the UK, or most other countries, for the SIAs and LEAs to be rigidly separated and there is a distinct need for the two branches of government to work more closely together. Some would say that in the UK, the separation of powers is not clear anymore with joint teams and joint working. However, it is still the case that the final arbiter of arrest, detention and prosecution rest with a completely separate part of the criminal justice system and not with the SIA.

The Parliamentary assembly of the European Council in 1999 (PACE 1402) and the UN report on safeguarding human rights while countering terrorism in 2010 (A/HR/14/46) suggests pre-trial investigation should be separated from the work of SIAs. This view is based on the fact that SIAs have wide ranging powers and methods which if used incorrectly would have a high impact on the human rights of a countries' citizens and could compromise the democratic process.

Whilst this may have been relevant when under discussion, things have moved on substantially since then. This is not only true in relation to increased threats to societies but also the rapid changes in technology. There was a time when only SIAs had access to certain intercept and intelligence gathering technologies. This is no longer the case. SIAs in most countries rely largely on commercial surveillance technologies which are available to everyone and used extensively by law enforcement and other government bodies. To say that SIAs may have a monopoly on wide ranging powers is no longer true. In addition, it is not just the SIAs who have the potential to abuse human rights and there are plenty of examples where countries without distinct intelligence/security services have seen their populations' human rights abused in other ways: e.g. through the military or Police services. Even with a separation of law enforcement and technical oversight, abuses can still occur.

In those countries where these powers are not separated, the system can work very well, such as the FBI in the USA.

From a UK perspective, with one of the oldest democratic security services, it is not so much the processes and laws that count but how they are applied. The biggest lessons are as follows:

- A clear written mandate as to what the SIA has responsibility for in terms of their investigations.
- Safeguards in place to ensure political neutrality (vetting of staff, no interference by government in appointment procedures or political appointees, clear staff guidelines on interaction with politicians, training on neutrality etc.)
- Clear separation between the people/departments/organisations investigating cases/operations in the first instance and those who will carry out the pre-trial investigations.
- An independent prosecuting authority which will take each case on its merits.
- Every prosecution case that results from an SIA investigation is placed before a criminal court with an independent judge who is in charge of how the trial is conducted. The court should have open proceedings so that justice is seen to be done with only a minimum of reporting restrictions, if any at all.
- An independent oversight system for the SIAs which covers executive, parliamentary, judicial, civil and internal elements.
- An independent body that reviews the most intrusive types of surveillance and ensures that the surveillance is fit for purpose and appropriate.
- An independent complaints body for the SIAs.
- Sophisticated legal departments (and to some extent independent) within the SIAs to advise the services.
- All staff are trained in their responsibility under the law and their ethical responsibilities in their work with regard to human rights and sanctions applied to those who misuse any powers.

Photo by Gorodenkoff, stock.adobe.com

Part IV:
DCAF recommendations

The case studies and thematic analyses in this publication demonstrate that democratic oversight of intelligence services especially those with law enforcement powers requires a comprehensive, multi-layered approach adapted to national contexts but grounded in common principles. Based on the findings, the following recommendations are proposed for policymakers, oversight bodies, and civil society actors across the Euro-Atlantic region:

Strengthen parliamentary oversight mandates and capacities

- ✔ Grant parliamentary committees clear legal authority to review classified material and conduct in-depth investigations into intelligence budgets.
- ✔ Ensure members of oversight committees receive specialised training in intelligence work, human rights law, and emerging technology issues.
- ✔ Provide independent research and legal support units to enhance analytical capacity and reduce reliance on government-provided information.
- ✔ Update legal frameworks to address new surveillance technologies, AI-driven analysis, and cross-border data flows.

Embed independent judicial review

- ✔ Require prior judicial authorisation for intrusive measures, such as surveillance, searches, and data interception, to ensure compliance with legality, necessity, and proportionality standards.
- ✔ Strengthen the ability of courts to review intelligence-led operations and remedies for individuals whose rights are infringed.

Enhance executive supervision with clear accountability lines

- ✔ Define and codify the respective roles of ministers, senior officials, and agency heads in setting strategic priorities and ensuring compliance with law and policy.
- ✔ Establish internal inspector-general or compliance offices with statutory independence to monitor adherence to mandates.

Institutionalise ombudsperson mechanisms

- ✔ Introduce or strengthen intelligence ombudspersons empowered to investigate complaints from the public, whistleblowers, and security sector personnel.
- ✔ Ensure these offices have direct access to agency records and decision-making processes.

Support civil society and media engagement

- ✔ Facilitate regular, structured dialogue between intelligence oversight bodies, civil society organisations, and investigative journalists, within appropriate security boundaries.
- ✔ Protect whistleblowers and journalists from retaliation when disclosing information in the public interest, in line with international standards.

Foster inter-Institutional cooperation

- ✔ Encourage coordinated oversight involving parliaments, judiciaries, executives, ombudspersons, and data protection authorities to close gaps and avoid duplication.
- ✔ Share best practices and lessons learned across Euro-Atlantic states through formal and informal networks.

Implementing these recommendations will not only improve accountability and public trust but also strengthen the operational effectiveness of intelligence services by ensuring they operate within clearly defined legal and ethical boundaries. In an era of complex security threats, oversight should be seen not as a constraint but as an essential pillar of resilient, legitimate, and democratic intelligence governance.

DCAF - Geneva Centre for Security Sector Governance
Chemin Eugène-Rigot 2E
1202 Geneva, Switzerland

+41 (0) 22 730 94 00
info@dcaf.ch

www.dcaf.ch