

PARLIAMENTARY OVERSIGHT OF MILITARY INTELLIGENCE



Dr Grazvydas Jasutis
Dr Teodora Fuior
Dr Mindia Vashakmadze



NATO PARLIAMENTARY ASSEMBLY
ASSEMBLEE PARLEMENTAIRE DE L'OTAN

DCAF

Geneva Centre
for Security Sector
Governance



About DCAF

DCAF - Geneva Centre for Security Sector Governance is dedicated to improving the security of people and the States they live in within a framework of democratic governance, the rule of law, and respect for human rights. DCAF contributes to making peace and development more sustainable by assisting partner states and international actors supporting them 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. Active in over 70 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. www.dcaf.ch.

Publisher

DCAF - Geneva Centre for Security Sector Governance

P.O.Box 1360

CH-1211 Geneva 1

Switzerland

info@dcaf.ch

+41 (0) 22 730 9400

Authors: Dr Grazvydas Jasutis, Dr Teodora Fuior, Dr Mindia Vashakmadze

Copy-editor: Tom Stanley

Design & layout: DTP Studio

ISBN: 978-92-9222-571-1

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. The NATO Parliamentary Assembly (NATO PA) and DCAF would like to thank all NATO PA Delegations who answered the surveys, the results of which served as a key resource for the analysis presented in this study. The authors also express sincere gratitude to Elizaveta Chmykh, Erlandas Snieskus, David Watson, Dragan Lozancic, Grzegorz Malecki, Henrik Bliddal, Richard Steyne, Roberta Calorio, Ruxandra Popa, Sarah-Claude Fillion, Steffen Sachs, Valérie Geffroy for their support and comments.

Notes

The opinions expressed in this publication are those of the authors and do not reflect the opinions or views of the Federal Department of Defence, Civil Protection and Sport (DDPS) of the Swiss Confederation.

The URLs cited in this document were valid at the time of publication. Neither DCAF nor the authors take responsibility for subsequent changes to any URLs cited in this publication.

@DCAF 2020. All rights reserved

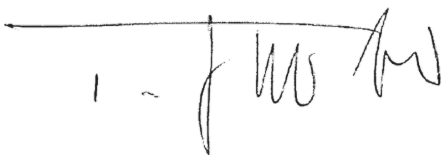
Forward

As a global center of excellence for security sector governance, DCAF - Geneva Centre for Security Sector Governance has worked for many years to improve security sector oversight. Much of this effort has been centered around cooperation with the NATO Parliamentary Assembly (NATO PA), under which DCAF has delivered joint trainings and seminars and conducted joint research along with the design and delivery of the so-called 'Oversight and Guidance' updates on parliament and relevant security sector developments. Alongside this, DCAF has produced several toolkits on overseeing the intelligence sector: an area of the security sector which has gained renewed attention in recent years. As the Director of DCAF, I am therefore extremely proud to present this study – one which seeks to expand the scope of our research to the area of military intelligence.

The study explores the evolution of military intelligence and its place within the broader framework of parliamentary oversight, identifies the key characteristics of military intelligence, and examines how these challenge efforts to institutionalize effective oversight over the activities of military intelligence agencies. Through a comparative analysis of existing practices in NATO member states with regard to oversight of military intelligence, the study demonstrates that oversight practices vary from state to state, and in general demands further attention.

The study is aimed at those responsible for the oversight of military intelligence, including parliamentarians and staffers, members of independent oversight bodies, researchers and civil society as well as individuals interested in security studies.

Working from the premise that all activities of democratic states should be open to parliamentary scrutiny, including military intelligence, DCAF and the NATO PA hope that this study will support efforts to advance oversight over military intelligence, and by extension, ensure that military intelligence agencies work in accordance with the principles of the rule of law and respect for human rights.



Thomas Guerber

Director, DCAF - Geneva Centre for Security Sector Governance

Preface

For twenty years, the NATO Parliamentary Assembly (NATO PA) has enjoyed a cooperative partnership with DCAF - Geneva Centre for Security Sector Governance, a cooperation supported by the Swiss government. Among others, this fruitful partnership has led to the publication of a series of “best practice” surveys on how parliaments in NATO members and partners address issues specific to the defence and security sector. Translated into several languages, these surveys have become important comparative studies for countries in transition towards stronger parliamentary oversight.

This study is the result of yet another joint NATO PA-DCAF project. Between February and August 2020, national delegations to the NATO PA were asked to answer a series of questions regarding the role and functions of their parliaments and parliamentary committees in overseeing military intelligence. The results of this survey served as a key resource for the analysis presented in this study.

As elected representatives of the people, parliamentarians have an essential role and responsibility in ensuring that security institutions remain effective, efficient, and accountable in their policies, actions, and use of public funds and that they implement the political goals set out by parliaments and governments. At the same time, parliamentarians must of course carry out these duties in a rigorous, non-partisan way and preserve the confidentiality necessary for these institutions to conduct their essential missions.

All oversight over institutions out of the public eye is difficult. However, it is perhaps most difficult when it comes to the military intelligence services. This study is an important contribution in an understudied field.

Together with DCAF, the NATO PA will continue to focus on parliamentary oversight as a key element in the shared, common value set that has made NATO the most successful alliance in history. We remain ready to assist countries seeking to enhance their parliamentary oversight practices.

A handwritten signature in blue ink, appearing to read 'R. Popa', with a long horizontal line extending to the left.

Ruxandra Popa

Secretary General

NATO Parliamentary Assembly



CONTENTS

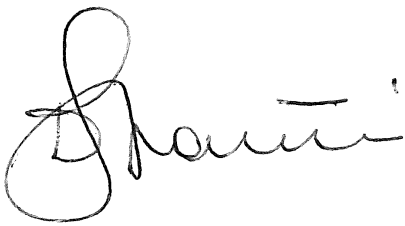
Introductory remarks	1
Executive summary	2
Chapter 1. Understanding Military Intelligence	4
Dr Grazvydas Jasutis, DCAF - Geneva Centre for Security Sector Governance	
Chapter 2. Parliamentary Oversight of Military Intelligence	17
Dr Teodora Fuior, DCAF - Geneva Centre for Security Sector Governance	
Chapter 3. Parliamentary Oversight of Military Intelligence Agencies: A Comparative Overview.....	40
Dr Mindia Vashakmadze	
Conclusion. Parliamentary Oversight of Military Intelligence: Recommendations	73
Dr Teodora Fuior, DCAF - Geneva Centre for Security Sector Governance	

Introductory remarks

While, in recent years, civilian intelligence agencies have been subject to increased parliamentary oversight, military intelligence remains terra incognita. With comparative literature on military intelligence limited, and little public knowledge on the sector, parliamentary committees and independent oversight bodies responsible for oversight of the security and defence sector often lack sufficient expertise and incentives to ensure effective oversight over military intelligence agencies. As the Assistant Director of DCAF – Geneva Centre for Security Sector Governance, it therefore brings me great pleasure to present this study, a cumulation of the joint efforts of my colleagues in DCAF Operations Europe and Central Asia, and our partners at the NATO Parliamentary Assembly.

The study examines the evolution of military intelligence and identifies the common characteristics of contemporary military intelligence agencies. It explores how these factors complicate efforts to ensure effective oversight over the military intelligence sector and outlines the main challenges to improving parliamentary oversight in this area. It concludes with a comparative analysis of existing practices in NATO member states in the area of military intelligence oversight, demonstrating that further work is needed to improve the legislative basis upon which such oversight is exercised.

This study demonstrates DCAF's firm commitment to ensuring that all areas of the security sector be open to parliamentary scrutiny and provides a valuable resource for those interested in advancing oversight over the conduct of military intelligence agencies.

A handwritten signature in black ink, appearing to read 'Darko Stančić', with a large, stylized initial 'D'.

Darko Stančić

Assistant Director & Head of Operations Europe and Central Asia

DCAF - Geneva Centre for Security Sector Governance

Executive summary

Effective parliamentary oversight of the activities of military intelligence agencies is complicated by several factors including: underdeveloped statutory regulations; the growth in the complexity and scope of military intelligence activities; dispersed administrative and management structures; the subordination of military intelligence agencies to respective Ministries of Defence and/or armed forces; and the limited knowledge of parliamentarians and staffers on such issues. Combined, these factors help account for the absence of research into military intelligence. As a result, a vicious cycle has emerged, with insufficient expertise and little public attention becoming mutually reinforcing; at once limiting access to the information necessary to increase expertise on overseeing military intelligence, while at the same time reducing incentives for conducting research into this area.

As a global center of excellence in the area of security sector governance, DCAF has for many years conducted joint research with the NATO PA, including in the design and delivery of the so-called 'Oversight and Guidance' updates on developments in the area of parliamentary oversight of the security sector. Alongside this, DCAF has produced several toolkits on overseeing the intelligence sector and is uniquely placed to contribute to research in the area of military intelligence.

Based on open research, and the results of surveys disseminated to delegations of the NATO PA, three subject-matter experts have contributed to this study. The first, Dr Grazvydas Jasutis, explores the evolution of military intelligence and its contemporary characteristics. The author concludes that the efforts of military intelligence agencies in NATO member states to respond and react to emerging security challenges has necessitated a re-examination of their traditional role of gathering information about enemy's doctrine, training, equipment and capabilities, to supporting national and multinational operations and responding to new domestic and external security challenges. NATO operations in Iraq, Kosovo and Afghanistan, as well as the security challenges originating from the East have revealed the need for a more adaptive and comprehensive approach by military intelligence. The author concludes that considering the growing need to cooperate and share capacities within and between intelligence services, a fusion of the functions of civilian and military intelligence might be considered. Such a fusion, it is argued, could facilitate inter-agency cooperation and subject both to enhanced parliamentary oversight.

The second expert, Dr Teodora Fuior, explores military intelligence within the broader framework of parliamentary oversight of the intelligence sector, providing practical examples and a useful checklist that can serve as a guide to exercising effective oversight.

The author explores the particularities of military intelligence, and how these complicate efforts to oversee it - even in comparison to other components of the intelligence sector. These include a sub-standard legal base, little public interest, and scarce open-source analysis and literature, resulting in insufficient overseer expertise and attention. A comprehensive review of the three main types of bodies mandated by parliaments to oversee military intelligence is presented and supported by references to different states' practice. Defence and security committees, intelligence oversight committees and non-parliamentary expert bodies are analyzed comparatively, with attention placed on the scope of their mandates and the advantages of each model. The author further reviews the main tools of parliamentary oversight (requesting reports, holding hearings, conducting field visits, and initiating special inquiries) and explains how they should be implemented in the oversight routine of a committee, pointing to practices that may be useful for engaging with military intelligence.

The third expert, Dr Mindia Vashakmadze, provides a comparative overview of existing practices in NATO member (and other) states as regards parliamentary oversight of mili-

tary intelligence. Based on the findings of surveys disseminated to NATO PA delegations in spring of 2020, the author demonstrates that the scope of parliamentary oversight of military/ defence intelligence agencies varies from state to state. In certain areas, parliamentary oversight remains weak, particularly in the areas of active intelligence operations as well as transboundary intelligence sharing and cooperation. The author differentiates between various components of oversight frameworks—both parliamentary and non-parliamentary—and points out that all levels of oversight are interconnected. He stresses that while both parliamentary and non-parliamentary oversight bodies play an important role in the overall oversight process, cooperation and coordination between the two could further be institutionalized and strengthened.

The last chapter, authored by Teodora Fuior, provides a review of strategies for improving the performance of parliamentary oversight of military intelligence. These range from clarifying the regulatory base of military intelligence and improving committee's access to information and expertise, to adopting detailed committee procedures and organizing joint action and cooperation among relevant oversight committees.

The study is aimed at all individuals and groups conducting research into the area of military intelligence, as well as those responsible for their oversight, including parliamentarians, staffers, researchers and civil society. Working from the premise that all activities of democratic states should be open to parliamentary scrutiny, including military intelligence, DCAF and NATO PA hope that this study will support their efforts to advance oversight over military intelligence, and by extension, ensure that they fully adhere to the principles of the rule of law and respect for human rights.

Chapter 1. Understanding Military Intelligence

Dr Grazvydas Jasutis, DCAF — Geneva Centre for Security Sector Governance

Introduction

Formulating a definition of intelligence for the security and defence sector is no easy task. Indeed, the product of such an effort is likely to have less value than the process of arriving at it, with definitions still contested within the research and practitioner community.¹ Arriving at a definition of military intelligence is an even more complicated process, owing primarily to the enigmatic and traditionally classified nature military intelligence operations. Despite this, in recent years governments have occasionally released information on such operations, indicating that the military intelligence services of NATO countries have been engaged in various missions.

For example, on 13 April 2018, the Netherlands Defence Intelligence and Security Service with support from the Netherlands General Intelligence and Security Service and counterparts from the United Kingdom, disrupted a cyber operation being carried out by a Russian military intelligence team. Information released by the Dutch government indicated that the operation had been conducted by entities within the Russian Federation (RF) and had attempted to target the Organisation for the Prohibition of Chemical Weapons located in The Hague.² In 2019, the Norwegian Military Intelligence released a report claiming that in recent years the RF has significantly strengthened its presence in the Arctic in recent years. Sources indicate that this development, as well as the more active behaviour of the military forces of the RF in the High North, looks set to continue and should be understood within the context of the RF's two long-term military objectives: securing natural resources and ensuring strategic stability. To this end, the use of "jamming" has become common place in recent use, with several cases of GPS jamming affecting Norwegian and NATO air traffic during the allied exercise Trident Juncture in the fall of 2018³.

In light of COVID-19, the director of the Military Intelligence Agency of Lithuania has underlined its readiness to assist the country's healthcare system in bolstering its medical intelligence capabilities in response to the lessons learned from the pandemic. By this, the director was referring to the role of military intelligence in providing analytical capabilities and assessments of medical and biological risks in the context of all threats and risks at the national level.⁴

On 17 January 2020, a little-known medical unit within the Canadian Forces Intelligence Command briefed Defence Minister Harjit Sajjan on COVID-19.⁵

¹ Central Intelligence Agency, 'A Definition of Intelligence', 1995, available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a08p_0001.htm.

² Government of the Netherlands, 'Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW,' 4 October 2018, available at: <https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw>.

³ High North News, 'Norwegian Intelligence Services Say Russian Build-Up in the North Continues', 12 February 2019, available at: <https://www.highnorthnews.com>.

⁴ The Baltic Times, 'Lithuanian health minister welcomes help from military intelligence', 1 June 2020, available at: https://www.baltictimes.com/lithuanian_health_minister_welcomes_help_from_military_intelligence.

⁵ CBC, 'Military intelligence unit briefed Sajjan on COVID-19 risk', 17 January 2020, available at: <https://www.cbc.ca/news/politics/military-intelligence-unit-covid-19-briefing-1.5657796>.

In contrast to other agencies, the United States Defense Intelligence Agency is fairly transparent, with their officials regularly reporting on their activities during public events disclosures. For example, its director, Lt. Gen. Robert P. Ashley, Jr., commented on Russian and Chinese Nuclear Modernization Trends at the Hudson Institute on 29 May 2019, openly stating that China is on course to double the size of its nuclear stockpile in the coming years: “We expect this modernization to continue and this trajectory is consistent with Chinese President Xi’s vision for China’s military, which he laid out at the 19th Party Congress and stated that China’s military will be “fully transformed into a first tier force” by 2050.”⁶

A certain level of transparency can also be observed in France, with its officials present during the “La Fabrique Défense” event, held 17-18 January 2020. The event was unprecedented in that it brought together members of the public and key officials from the military establishment, including military intelligence agency officials, to “inform, discuss and debate”.⁷ Traditionally less inclined to engage with the public, the UK’s Defence Intelligence Agency has made efforts in recent years to increase their transparency. Tasked with monitoring global instability and tracking threats to the UK, amongst other things, its analysts provide advice to senior officials, shaping the Government’s approach to emerging threats and supporting UK forces deployed across the globe.⁸

There is limited information in the academic and specific literature focused on military intelligence and their role in contemporary security structures. J. Moran examined the use of military intelligence in aiding civil power in England and Wales, highlighting the extent to which its commanders were developing principles of military intelligence years before any formal doctrine was created.⁹ R. Best described the role of military intelligence in NATO operations in Kosovo, the importance of intelligence to current and future military operational capabilities, and the challenges facing the U.S. Intelligence Community in supporting such operations. His analysis claims that NATO’s bombing campaign in Kosovo and Serbia - resulting in Serbian withdrawal and very few allied casualties - was a result of the use of precise munitions as well as the military intelligence capabilities acquired by U.S. forces in the 1990s. At the same time, he notes that such resources are finite, and should large-scale inter-state hostilities occur, may not be adequate on their own.¹⁰

D. Charters analyzed the role of Canada’s Military Intelligence Agency (CF MI) in Afghanistan, posing two fundamental questions: how did the CF MI adapt to their mission, and did it fulfill its operational responsibilities? He concluded that it adapted by drawing upon relevant operational military intelligence experience from post–Cold War peace support and stability operations by adapting structures and doctrines designed for conventional war, and by learning from current operations. He also noted that the CF MI adapted effectively at the tactical level, providing reliable intelligence to forces tracking insurgents and locating Improvised Explosive Devices.

⁶ Defense Intelligence Agency, ‘DIA Statement on Lt. Gen. Ashley’s Remarks at Hudson Institute’, 13 June 2019, available at: <https://www.dia.mil/News/Speeches-and-Testimonies/Article-View/Article/1875351/dia-statement-on-lt-gen-ashleys-remarks-at-hudson-institute/>.

⁷ Ministère de la Défense, ‘Participation de la DRM à La Fabrique Défense’, 29 Janvier 2020, available at: <https://www.defense.gouv.fr/english/ema/transformation/actualites/participation-de-la-drm-a-la-fabrique-de-fense>.

⁸ Wiredgov, ‘Chief of Defence Intelligence comments on threats the UK will face in coming decades’, 14 September 2020, available at: <https://www.wired-gov.net/wg/news.nsf/articles/Chief+of+Defence+Intelligence+comments+on+threats+the+UK+will+face+in+coming+decades+14092020111000?open>.

⁹ J. Moran, ‘British military intelligence in aid of the civil power in England’, 2018 and Wales’, *Journal of Intelligence History*, 17:1, p. 1-17.

¹⁰ CRS Report for Congress, ‘Kosovo: Implications for Military Intelligence’, 5 November 1999, available at: https://www.everycrsreport.com/files/19991105_RL30366_fb37a2ab7103f2cb51abadd9b733cdba2110a286.pdf.

Despite this positive appraisal, his analysis also demonstrated that providing commanders and their personnel with the situational awareness required to understand the complex factors sustaining the insurgency was a major challenge. This, along with other factors, helped explain the difficulty of the Canadian Armed forces in containing the spread of the insurgency within its area of operational responsibility.¹¹

M. Bang researched intelligence assessments and the activities of intelligence agencies, applying the case study of Swedish Military Intelligence Agency work in Afghanistan between 2008 and 2012.¹² One of the most influential papers on military intelligence was prepared by senior US intelligence officers and entitled 'Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan'. In it, they argued that although the US focused the overwhelming majority of collection efforts and analytical brainpower on insurgent groups, its intelligence apparatus were still unable to answer fundamental questions concerning the environment in which these groups operate, and in particular how to effect behavioural change at the community level. They quoted General Stanley McChrystal's now infamous words: "Our senior leaders – the Chairman of the Joint Chiefs of Staff, the Secretary of Defense, Congress, the President of the United States – are not getting the right information to make decisions ... The media is driving the issues. We need to build a process from the sensor all the way to the political decision makers."¹³ The paper was critiqued by Leo Blanken & Justin Overbaugh, who argued that the report sought to expand the substantive tasks of the military intelligence practitioner, while collapsing nontrivial aspects of existing organizational hierarchies. In it, they claimed that the implementation of the Flynn Report's proposals would match poorly with the traditional nature of military intelligence and the realities of human resources constraints. Further, the resulting scale of unfiltered data such a system would produce might serve to overwhelm rather than assist decision makers. Finally, they concluded that the problems expressed in the Flynn Report should not be traced to the military intelligence apparatus per se, but rather to the inability of US political leadership to map out a clear vision for current operations – both in Afghanistan, and in the counterinsurgency environment in general.¹⁴

An occasional paper by RAND examined how military intelligence organizations and, more broadly, the defence intelligence enterprise approaches the task of all-source fusion analysis. It recommended a paradigm shift not only in the approach that the military takes to all-source fusion but also in the way that the services and US Department of Defense intelligence agencies recruit, train, educate, and promote their analytic workforces¹⁵. S. Ashley, T. Murali and J. McEachen reviewed documented problems in military intelligence that appear well suited for improvement via blockchain technology. As data sources diversify, questions of the validity and accuracy of incoming data continue to arise. Carefully implemented, blockchain technology might enable us to weed out data from miscalibrated sensors or even deceptive adversary activity.¹⁶ E. Pecht and A. Tishler developed a dynamic

¹¹ Charters A D 'Canadian Military Intelligence in Afghanistan. *International Journal of Intelligence and Counter Intelligence*', 2012, 25:3, p. 470-507.

¹² M. Bang 'Institutional influence on assessments: the institutional analysis and development framework applied to military intelligence', *The International Journal of Intelligence, Security, and Public Affairs*, Volume 20, 2018, Issue 1, p. 47-70.

¹³ M.T. Flynn, M Pottinger, D P. Batchelor, 'Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan', January 2010, available at: https://online.wsj.com/public/resources/documents/AfghanistanMGFlynn_Jan2010.pdf.

¹⁴ L. Blanken, J. Overbaugh, 'Looking for Intel? ... or Looking for Answers? Reforming Military Intelligence for a Counterinsurgency Environment', *Intelligence and National Security*, 2012, 27:4.

¹⁵ RAND 'Military Intelligence Fusion for Complex Operations A New Paradigm', 2012, available at: https://www.rand.org/pubs/occasional_papers/OP377.html.

¹⁶ S. Ashley, T. Murali, J. McEachen (2019), 'Military Intelligence Applications for Blockchain Technology. Proceedings of the 52nd Hawaii International Conference on System Sciences', available at: <https://pdfs.semanticscholar.org/8c8d/8c8d8c8d8c8d8c8d8c8d8c8d8c8d8c8d.pdf>.

model that integrates military intelligence into the defence capability of the country and the optimal allocation of its budget. They asserted that the effectiveness of the country's military intelligence was contingent on the quality of its human capital, which, in turn, implies a long-term positive relationship between the government's various civilian expenditures and its capacity to achieve a cost-effective intelligence and, hence, military capability.¹⁷ C. Mole has analyzed how philosophy – in particular, epistemology – has contributed to the analysis of criminal and military intelligence.¹⁸

The focus and limited scope of existing literature on military intelligence demonstrates that it remains enigmatic, and that the role of military intelligence in national security structures requires further attention. To this end, this paper seeks to assess the functionality of military intelligence in the contemporary security environment. It is composed of three parts: the first addresses the traditional mandates of military intelligence agencies; the second explores their capabilities to address broader security challenges; while the third proposes a model for the fusion of military and civilian intelligence services that has gained traction in recent years.

The paper is based on interviews with former and current military intelligence officers and relies heavily on open-source research, documentation and media reports. It does not claim to cover all aspects of the role of military intelligence, but rather to demonstrate the evolution of the military intelligence, and the emerging issues that impact the missions of military intelligence agencies working in the contemporary security environment.

1. Understanding military intelligence and its functions

According to NATO Allied Joint Publication-01, dated February 2017, the intelligence is the product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision makers.¹⁹ From time immemorial, intelligence has been a key factor in security planning, as reflected in the biblical story of the 'twelve spies' and Sun Tzu's treatise *The Art of War*.²⁰ R. Clark has stated that intelligence as process is exemplified by the so-called intelligence cycles. The classic intelligence cycle begins with requirements, followed by information collection, processing and analysis of such information, and distribution of the final product (intelligence) to those individuals or organizations that requested it, or who need it and have received the appropriate authorization to receive it.²¹ The same cycle holds for military intelligence at the tactical, operational and strategic level. Hence, military intelligence is essentially the process of data collection and knowledge analysis for decision-making by military and governmental hierarchies. Generally, military intelligence is operated and controlled by governmental (or military) agencies and is used to assess the capabilities and intentions of adversaries, and to increase the

ticscholar.org/4db1/edd97c5867ced07692e4c1e277c0fa3205ae.pdf.

¹⁷ E. Pecht, A. Tishler 'Budget allocation, national security, military intelligence, and human capital: a dynamic model', *Defence and Peace Economics* 2015.

¹⁸ C. Mole, 'Three Philosophical Lessons for the Analysis of Criminal and Military Intelligence. *Intelligence and National Security*', 2012, 27:4.

¹⁹ NATO Allied Joint Publication-01 (AJP-01), February 2017, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/905877/20200728-doctrine_nato_allied_joint_doctrine_ajp_01.pdf.

²⁰ E. Pecht, A. Tishler, 'The Value of Military Intelligence', 2011, *Defence and Peace Economics*, 26(2).

²¹ R. Clark, *Intelligence and National Security: A Reference Handbook*, Greenwood Publishing Group, 2007, p. 12.

effectiveness of the country's own weapon systems.²² E. Pecht and A. Tishler offer the following characteristics of military intelligence:²³

- Military intelligence in and of itself has no direct effect on military capability. To be effective, military intelligence must be integrated with weapon systems and personnel in order to support military capabilities.
- Intelligence consists of collecting and assessing knowledge which is relevant to all levels of military and government hierarchies – state leaders, policy makers, senior military personnel and soldiers. Such intelligence may be used to support both tactical and strategic decision-making.
- Gaining information superiority is based on high-quality human capital and technology. Human capital characteristics such as entrepreneurship and innovation are the key factors defining the success and effectiveness of the intelligence community. Moreover, most of the relevant intelligence cannot be bought, as it concerns the country's particular rivals and needs. Thus, it must be produced, with each country needing to therefore invest their own resources. In other words, each country has to produce its own military R&D and internal sources and capabilities for collecting, analyzing and distributing the necessary data to the relevant agents at the relevant time.
- The intelligence mission is hampered by an inherent uncertainty, which may be reduced by good procedures and high-quality human capital but cannot be eliminated.
- Intelligence gathered by 'rivals' may have a significant negative influence on the country's military capability. Effective intelligence gathering by such rivals can reduce the relevance of the country's own intelligence as well as the potency of its weapon systems and, thus, its overall military capability. Strategically, a higher relative level of intelligence is likely to lead to military superiority and better deterrence.

In general, military intelligence is mainly composed of six elements:

- Open-source intelligence (OSINT) – the collection and analysis gathering of information from public and open sources.
- Human intelligence (HUMINT) – a category of intelligence derived from information collected and provided by human sources.
- Imagery intelligence (IMINT) – the collection of information on objects produced electronically or by optical means on film, electronic display devices, or other media. Imagery can be derived from visual photography, radar sensors, infrared sensors, lasers, and electro-optics.
- Measurement and signature intelligence (MASINT) – scientific and technical intelligence information obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender and to facilitate subsequent identification and/or measurement of the same.²⁴

²² E. Pecht, A. Tishler, 'Budget allocation', 2011, Defence and Peace Economics.

²³ E. Pecht, A. Tishler, 'The Value of Military Intelligence,' 2011, 26(2).

²⁴ FAS, 'Measurement and Signature Intelligence (MASINT)', available at: <https://fas.org/irp/program/masint.htm>.

- Geographic intelligence (GEOINT) - the product arising from the collection, processing, analysis, evaluation, and interpretation of geographical information, concepts, and theories about foreign or domestic entities or geographical areas.²⁵
- Signals intelligence (SIGINT) – the information received from electronic signals and systems used by external targets, such as communications systems, radars, and weapons systems.

Of note, some countries have created cyber or digital network intelligence (CYBINT/DNINT) that include the information received from cyberspace.

The development and organization of intelligence agencies dates to the end of the 19th century, when they began to emerge as governmental advisory units or as integral components of the military. Military intelligence gained traction in World War II and the Cold War era, and thus also in prominence within the security and defense sector.²⁶ The role of military intelligence in conflicts first became apparent during the aftermath of WW2, particularly in British-controlled Palestine, and was subsequently reinforced in Kenya and Malaya, where military intelligence was seen as an important factor in the campaigns against the Mau Mau and Chinese Malayan National Liberation Army, respectively.²⁷ The US Defense Intelligence Agency (DIA) was also active during the Cold War, and played a particularly important role in the Cuban Missile Crisis. By September 1962 DIA analysts suspected that the Soviet Union had placed nuclear-capable missiles in Cuba. The then director of the DIA, Lt. Gen. Joseph F. Carroll, established the Cuban Situation Room on Oct. 4, 1962, so that the agency could provide 24-hour coverage on the crisis and support military contingency planning.²⁸ The traditional functions and role of military intelligence generally follow these trends, and as such are clear and well defined.

Blanken and Overbaugh note that during the Cold War, military intelligence analysts relied heavily on a process of deduction to produce intelligence.²⁹ For example, in preparation for the possibility of a major conventional conflict with countries within the Warsaw Pact, intelligence collectors during the Cold War gathered information about Soviet doctrine, training, equipment and capabilities that was then collated into an 'order of battle' (OB). This OB was used to create a common 'threat template' that could be used for deductive analysis by both senior and junior personnel to create intelligence products for commanders. Based on the information contained in the OB, analysts would then collect reports from the battlefield and make reasonable conclusions about the situation on the ground. For a heuristic example, from the placement of an enemy reconnaissance vehicle the location of the main attack force, headquarters element, and supply chain could be deduced. Analysts cross-referenced reports with known enemy doctrine and were able to create a somewhat reliable picture about the enemy's disposition, capabilities, and intentions.³⁰ While the tactics and methods used by military intelligence agencies remained fairly consistent throughout the Cold War, Operation Desert Storm in Iraq brought about large changes.

²⁵ WJ. Crampton, 'Geographical Intelligence', 19 December 2016, available at: <https://www.oxfordbibliographies.com/view/document/obo-9780199874002/obo-9780199874002-0059.xml#:~:text=Geographical%20intelligence%20is%20the%20product,domestic%20entities%20or%20geographical%20areas.&text=This%20has%20meant%20an%20increased%20role%20for%20human%20geography%20concepts%20and%20information.>

²⁶ E. Pecht, A. Tishler, 'The Value of Military Intelligence', 26(2).

²⁷ TR. Mockaitis, 'Epilogue: The Lessons of British Counterinsurgency', in: *British Counterinsurgency, 1919–60. Studies in Military and Strategic History*, Palgrave Macmillan, 1990, London.

²⁸ Defense Intelligence Agency, 'DIA's role during the Cuban Missile Crisis', 20 October 2014, available at: [https://www.dia.mil/News/Articles/Article-View/Article/567027/dias-role-during-the-cuban-missile-crisis/.](https://www.dia.mil/News/Articles/Article-View/Article/567027/dias-role-during-the-cuban-missile-crisis/)

²⁹ L. Blanken, J. Overbaugh, 'Looking for Intel', 27:4.

³⁰ Ibid.

The US Congress report 'Intelligence Successes and Failures in Operations Desert Shield/Storm' revealed that intelligence agencies had extensive knowledge on the units, locations and equipment of Iraqi troops (but not the numbers of troops) deployed to face coalition forces, despite Iraq's high-level communications security and a US-imposed ban on overflying Kuwait before the air war began. In general, the national intelligence community mobilized in support of Operation Desert Storm. Still, some national intelligence agencies appeared unfamiliar with or unresponsive to the intelligence needs of the warfighting commanders. Some senior CENTCOM commanders were unfamiliar with the capabilities and limitations of US intelligence systems. At the time of the invasion, CENTCOM had few trained personnel, no collection assets under its direct control and no joint intelligence architecture to guide the buildup of in-theater intelligence capabilities.³¹ Rectifying these issues became critical for improving the coordination and overall communication within the intelligence community.

Another important development in military intelligence stems from the NATO operation in Kosovo. The Kosovo campaign depended upon intelligence from a variety of sources. SIGINT collected by manned aircraft and unmanned aerial vehicles (UAVs) were used by NATO commanders to direct attacks by allied aircraft operating over Kosovo and Serbia. To facilitate attacks on stationary installations (in both Kosovo and Serbia proper) video images were fused with digital terrain elevation data provided from national satellites. This data was used to target cruise missiles launched by submarines in the Adriatic and by B-1 bombers operating from bases in the United States.³² The effective use of intelligence in Kosovo in large measure resulted from lessons learned in the Persian Gulf War of 1991. Desert Storm had seen national intelligence systems successfully supporting tactical operations and the emerging importance of precision guided weapons. The air campaign revealed many shortcomings, however, in facilitating the rapid use of large quantities of information. One Air Force historian described the "difficulty of melding the US Air Force planning, operations, and intelligence functions into a smoothly functioning team" as a "potentially grave organizational flaw."³³ Of equal importance is the creation of an integrated intelligence "grid" that can be directly accessed by warfighters at national, operational, and tactical levels. Information from the grid is then fed directly into weapons systems.³⁴

Since September 11, there has been a move for military intelligence operations to encroach upon areas traditionally occupied by internal security services and external intelligence services. This has been due to the increased risk of terrorism and the role of non-state actors in threats to the state, such as Al-Qaeda and ISIS. This required an overseas military response in addition to intelligence gathering. Many countries have seen an increased role for tactical units as they become involved in both tactical and strategic collection of intelligence. The UK had experienced this step change earlier in Northern Ireland where all the intelligence agencies were operating and often competed for resources and operations alongside military intelligence units.

The recent conflicts in Iraq and Afghanistan ushered in new challenges for the military intelligence community. While in the past, the debate on intelligence was of a purely technical and military character, questions began to rise as to why intelligence services seemed ineffective in providing timely intelligence to policy makers, and how analysis and input to policy could be more efficient.³⁵ To this end, the RAND report 'Military Intelligence Fusion for Com-

³¹ U.S. House of Representatives Committee on Armed Services, 'Intelligence Successes and Failures in Operations Desert Shield/Storm', 6 August 1993, available at: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a338886.pdf>.

³² CRS Report for Congress, 'Kosovo: Implications for Military Intelligence', 5 November 1999, available at: https://www.everycrsreport.com/files/19991105_RL30366_fb37a2ab7103f2cb51abadd9b733cdba2110a286.pdf.

³³ Ibid.

³⁴ Ibid.

³⁵ G. Erikkson, Swedish Military Intelligence Producing Knowledge, Swedish National Defence College, Edin-

plex Operations' straightforwardly placed the blame on military intelligence, accusing them of failing to provide commanders and policymakers with an effective understanding of complex counterinsurgency (COIN) environments. This failure was argued to result in part from the failure to deliver holistic, fused analysis.³⁶ Most analyses of complex environments are derived from a systems analysis model that artificially deconstructs both the environment and the people and groups within it. Treating complex environments, such as Iraq or Afghanistan, as a system that can be broken into simply labeled component parts leads analysts to make unhelpful and logically unsound assumptions regarding human identity. These assumptions, in turn, undermine analytic effectiveness. Instead of fusing available information in a way that accurately reflects the inherently complex "shades-of-gray" ground truth, military analysts—influenced by systems analysis and conventional military doctrine—often channel their thinking and efforts into three artificially color-coded categories: red, white, and green. These colors represent, respectively, the enemy, the population, and the host nation. For example, the military operation in Iraq (in 2003) resulted in the removal of Saddam Hussein. However, the inability to integrate and assess information on civilian aspects of the situation on the ground significantly prolonged the operation and did not create conducive security in Iraq. On the other hand, to put military failures at the hands of intelligence is not accurate, as the greater reason is that of the failure to engage in any way other than militarily with the local population to solve insurgency in a complex environment.

The military intelligence community was also shaken by the so-called Flynn report, produced by Major General Michael T. Flynn, former Deputy Chief of Staff of Intelligence (CJ2) for the International Security Assistance Force in Afghanistan. In it, he noted that eight years into the war in Afghanistan, the US intelligence community was only marginally relevant to the overall strategy.³⁷ As mentioned above, the report argued that although the US focused the overwhelming majority of collection efforts and analytical brainpower on insurgent groups, its intelligence apparatus were still unable to answer fundamental questions concerning the environment in which they operate, and in particular how to effect behavioural change at the community level. Unaware of local economics and landowners, ill-informed about powerbrokers and how they might be influenced, disinterested in correlations between various development projects and the levels of cooperation among villagers, and disengaged from those most able to answer such questions – whether aid workers or Afghan soldiers – US intelligence officers and analysts were unable to provide the knowledge, analysis and information necessary for high level decision-makers to wage a successful counterinsurgency. Some of these issues have been echoed by D. Charters, who analyzed the Canadian military intelligence in Afghanistan and stated that providing commanders and their personnel with the situational awareness required to understand the complex factors sustaining the insurgency was a major challenge.³⁸

Recently, NATO and its allies have had to respond to the challenges from the East. In particular the so-called Gerasimov Doctrine which talks of "total war", where all means are used to de-stabilize an enemy (e.g., political, hacking, economic, disinformation, industrial espionage, asymmetrical warfare). Whether a true doctrine or not, the response by the western defence community has been to see all of the activities contained in the doctrine as being part of military responsibility. This has put matters such as political espionage under the focus of military engagement. The Russia dimension has also contributed to this change of focus due to the increased activity of the GRU (the Main Directorate of the General Staff of

burgh University Press, April 2017, p. 1-19.

³⁶ B. Connable, 'Military Intelligence Fusion for Complex Operations A New Paradigm', Rand, 2012, available at: https://www.rand.org/pubs/occasional_papers/OP377.html.

³⁷ MT. Flynn, M. Pottinger, DP Batchelor, 'Fixing Intel'.

³⁸ AD. Charters, 'Canadian Military Intelligence in Afghanistan', *International Journal of Intelligence and Counter Intelligence*, 2012; 25:3, p. 470-507.

the armed forces of the Russian Federation) who had traditionally been focused on defence intelligence but has become an arm of general intelligence activity in preference to the traditional SVR (Foreign Intelligence Service of the Russian Federation) and FSB (Federal Security Service). This change has also prompted changes in attitude within defence ministries and the feeling that intelligence in a more general sense was not part of their remit.

2. Challenges of military intelligence

The Flynn report reverberated across the academic community and stimulated increased research into the area of military intelligence. The concerns were based both on the duties tasked to military intelligence practitioners, as well as the structural organization of military intelligence. In particular, the Flynn Report argued for an expansion of substantive duties, as well as the collapsing, to some degree, of the chain of command within the military–political structure. In his view, while this would improve the effectiveness of military intelligence, it would also risk an undifferentiated deluge of data flowing upwards to higher-level decision makers.³⁹

In his report, Maj. Gen Flynn complained that military intelligence remained too enemy-centric. The intelligence community's standard mode of operation is somewhat passive when aggregating information that is not enemy-related and relaying it to decision makers or fellow analysts. It is a culture that is dislocated from how its analytical products, as they now exist, actually influence commanders.⁴⁰ Flynn also noted how information collection during a counterinsurgency differs from information gathering in a conventional war.⁴¹ In a conventional conflict, ground units depend heavily on intelligence from higher commands to help them navigate the fog of war. Satellites, reconnaissance planes, and more arcane assets controlled by people far from the battlefield inform ground units about the strength, location, and activity of the enemy before the ground unit even arrives. Information flows largely from the top down.⁴² In a counterinsurgency however, the flow is (or should be) reversed. The soldier or development worker on the ground is usually the person best informed about the environment and the enemy. As a result, Provincial Reconstruction Teams (PRTs), and those on the ground bear a 'double burden' in a counterinsurgency: they are at once the most important consumers and suppliers of information.⁴³ This assessment provoked many questions among the intelligence and research community, such as what qualities for a military intelligence officer are needed to gather community-centric information, how to deal with an immense amount of diverse information, and whether this information actually supports decision-making.

The nature of counterinsurgency operations suggests that the functions and duties of military intelligence could be expanded to make the intelligence more community-centric. The current pandemic and the emergence of new security challenges necessitate an adaptive approach and changes within the intelligence services, including military intelligence. The expansion of duties and tasks of any organization (especially a military one) needs to be carefully considered from financial, legal and oversight perspectives. While these aspects are covered in the further articles of this publication, attention should be paid to the impact of internal organizational changes within a military organization. For example, the main task of the Military Intelligence of Czech Republic is to collect and evaluate information important for the defence of the country. It integrates both intelligence and counter-intelligence activity; provides information both domestically and abroad; focuses on information about

³⁹ L. Blanken, J. Overbaugh, 'Looking for Intel', 27:4.

⁴⁰ MT. Flynn, M. Pottinger, DP Batchelor, 'Fixing Intel'.

⁴¹ Ibid.

⁴² Ibid.

⁴³ Ibid.

intentions and activities threatening classified information and directed against the defence of the Czech Republic; and also monitors the activities of foreign intelligence services in the field of defence. On the basis of its commitment to NATO to build national capacity in the field of imagery intelligence, its military intelligence agency is establishing the satellite center SATCEN CR.⁴⁴ These traditional functions performed by the military intelligence could be influenced by various factors and uncertainties in the security field. For example, in light of COVID-19, the military intelligence agencies of several NATO countries have been engaged in the mitigation of risks, requiring a more adaptive approach and possibly internal changes (i.e., employment of medical experts). Questions remain as to whether or not military intelligence officers are ready to process information on the impact of social, economic, cultural and political issues on a country's defence structure, as well as the terabytes of information now available, in order to adequately support decision makers.

In order to answer these questions, one must first start from the premise that new functions and new challenges require varied and diverse expertise. According to Blanken and Overbaugh, current military intelligence soldiers are trained in a narrow set of skills. For example, analysts are not trained to be subject matter experts in any field and may lack skills in different areas. Current military analyst training normally begins with the basic training necessary to acquire tactical skills, followed by several months of training in their respective MOS (military occupation specialty) which is designed to provide enlistees with a basic level of proficiency in a given subject.⁴⁵ For example, the US army advertises the role of intelligence analyst as someone primarily responsible for the analysis, processing and distribution of strategic and tactical intelligence.⁴⁶ Such roles are integral to providing Army personnel with information about enemy forces and potential battle areas. The job duties are more specific and include the following: prepare all-source intelligence products to support the combat commander; assess the significance and reliability of incoming information with current intelligence; and establish and maintain systematic, cross-referenced intelligence records and files. Interestingly, the advertisement also notes that the training involves other elements, including critical thinking, the preparation of maps, charts and intelligence reports, the understanding of military symbology and the use of computer systems. However, it remains unclear as to whether this job description corresponds to the need for a more adaptive and holistic role for military intelligence. To focus on community-centric military intelligence and furthermore to develop proactive military intelligence products, which respond to the current and future security challenges, experts with very diverse skills are required. For example, cyber threats to NATO are becoming more frequent, complex, destructive and coercive. NATO and its allies continue to rely on strong and resilient cyber defences to fulfil the Alliance's core tasks of collective defence, crisis management and cooperative security.⁴⁷ We must consider the role military intelligence can play in dealing with the growing sophistication of the cyber threats and attacks it faces.

Nowadays, all operations tend to incorporate cyber dimensions, thus exponentially increasing the need for a diversity of skills and knowledge. An ideal military intelligence officer should be required to collect, analyze and disseminate critical and diverse information, participate in reconnaissance missions, and provide intelligence support to the armed forces and multinational military forces. It is critical that the officer be able to navigate through large amounts of data information related to cyber defence, pandemics, religious fundamentalism, economic challenges, human rights violations, and other crises in order to support the decision-making process. To this end, the ability to process and navigate through large

⁴⁴ Military Intelligence of the Czech Republic, Home Page, available at: <https://www.vzcr.cz/en/who-we-are-60>.

⁴⁵ L. Blanken, J. Overbaugh, 'Looking for Intel', 27:4.

⁴⁶ US Army, 'Careers and jobs', available at: <https://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/intelligence-and-combat-support/intelligence-analyst.html>.

⁴⁷ NATO, 'Cyber defence', 2020, available at: <https://www.nato.int/cyberdefence/>.

amounts of data has become a key requirement for military intelligence officers, as noted in Maj. Gen Flynn's report. Flynn notes that in Afghanistan, military intelligence lacked analysts who were able to produce quality assessments on issues including census data and patrol debriefs; minutes from meetings with local religious and tribal leaders; after-action reports from civil affairs officers and PRTs; polling data and atmospheric reports from psychological operations and female engagement teams; and translated summaries of radio broadcasts that influence local communities, not to mention the field observations of Afghan soldiers, UN officials, and non-governmental organizations⁴⁸. This vast and underappreciated body of information, almost all of which is unclassified, offers few clues about where to find insurgents, but does provide elements of even greater strategic importance – a map for leveraging popular support and marginalizing the insurgency.⁴⁹ The intelligence collected may be needed for tactical and operational purposes, or for defence of the country and partner countries. The community-centric approach in operations or defence-centric intelligence (which is a rather vague and broad perception of tasks entrusted to military intelligence) widely expands the scope and requirements to process a large amount of information from various sources.

Having explored the need for more diverse expertise within military intelligence and enhanced abilities to process large amounts of information, sources also suggest the need to master modern technologies, delineate functions and ensure clear tasking. As technology has progressed, the variety of resources that contribute to the intelligence process has grown.⁵⁰ Data sources include manned and unmanned space, airborne, ground, maritime, and cyberspace platforms with any variety of sensors, resulting in large amounts of data. Therefore, blockchain technology could be used to integrate and process the information and identify and remove data from miscalibrated sensors or even deceptive adversary activity.⁵¹ Furthermore, political leadership in general and the national parliaments in particular should make clear the tasks that military intelligence are requested to perform. Assignments, benchmarks, results and expectations need to be realistic and correspond to the capacities of military intelligence services.

As military intelligence agencies are requested to support decision makers through gathering information in a complex environment, it has become increasingly difficult to draw the lines between military and civilian intelligence services. This leads to another option to be considered - the fusion of military and civilian intelligence agencies.

3. The fusion of military and civilian intelligence

A fusion of military and civilian components in the security domain could be common practice as the lines between civilian and military functions become blurred. At the Warsaw Summit in July 2016, NATO Heads of State and Government agreed to establish a new Joint Intelligence and Security Division (JISD) in order to improve NATO's ability to draw on a wide range of intelligence resources. JISD is led by an Assistant Secretary General for Intelligence and Security, and consists of two pillars: intelligence (with the merged strands of military and civilian intelligence); and security (the NATO Office of Security).⁵² As a matter of principle, the possible fusion (or dense coordination) of military and civilian intelligence services at the national level could also be considered. Both rely on similar measures and methods; however, their areas of responsibilities and types of consumers of their informa-

⁴⁸ MT. Flynn, M. Pottinger, DP Batchelor, 'Fixing Intel'.

⁴⁹ Ibid.

⁵⁰ S. Ashley, T. Murali, J. McEachen, 'Military Intelligence Applications for Blockchain Technology'.

⁵¹ Ibid.

⁵² NATO, 'Joint Intelligence and Security Division (JISD) – Intelligence Production Unit (IPU)', 3 March 2017, available at: <https://www.nato.int/cps/fr/natohq/107942.htm>.

tion differ. Military intelligence concerns the procurement of information and/or execution of tasks mainly involving other countries' military forces, plans, and operations, which support the commander or senior defence leadership to make an informed decision. Civilian intelligence agencies, on the other hand, primarily gather information and/or execute tasks concerning political, economic and other strategic areas of interest.

The advantages of the fusion of civilian and intelligence agencies include the following:

- **Closer interagency cooperation:** Considering the increasingly complex nature of security risks and threats faced by states, the fusion of civilian and intelligence agencies would lead to closer cooperation, which could be used to assess various contexts and produce reliable outcomes based on joint civil-military assessments.
- **Competition:** A reduction in competition, which commonly exists between intelligences services, would have a positive impact on overlapping areas of responsibility. Moreover, a single intelligence organization could quickly move its resources and assets to where they are needed the most, regardless of whether they are civilian or military.
- **Cost benefits:** Fusion would reduce costs and save resources for operational needs, including field agents and assets, analysts and support staff, as well as technology, logistics and maintenance, research, training and other support functions. It would also reduce the number of documents produced for the top level and the need for representatives in foreign countries.

However, fusion could also result in negative consequences, including:

- **Relationships between military intelligence and armed forces:** It could increase the likelihood of alienating military intelligence officers from the armed forces. The consequences could be manifold, including the degradation of military skills, expertise and knowledge, as well as adverse effects on recruiting and professional development (military promotions, rank, etc.).
- **Defence and military requirements:** The intelligence collected and produced may not fully meet defence and military requirements.
- **Civil-military tensions:** Possible polarization along civil-military lines, could lead to conflicts and confrontations that affect organizational harmony. For example, military experts could object to civilian infringements in what they believe to be purely military matters. On the other hand, civilians would be objecting to what they perceive as military meddling in purely non-military areas of expertise.
- **Simplification and loss of perspective:** Unification of the narrative and stream of analysis could provoke simplification of the picture consumers obtain, and the loss of different perspectives.
- **Chain of command and management:** Fusion could result in an increased complexity within the chain of command, as well as more complicated and less effective management of the organization. The integration of military culture into the civilian organization may also cause internal frictions.
- **Military capacities:** Fusion could lead to decreased military capacities to conduct operations in high-risk areas due to limited military intelligence capabilities.

Conclusion

Military intelligence service remains one of the most clandestine organizations within the defence sector, and their functions vary from country to country. Considering the increasingly complex nature of security risks and threats faced by NATO states, military intelligence services have attempted to respond and react to the emerging security challenges. However, this has necessitated a re-examination of their traditional role - from gathering information about an enemy's doctrine, training, equipment and capabilities that was then collated in the enemy 'order of battle', to supporting national and multinational operations and responding to new domestic and external security challenges. The major NATO operations in Iraq, Kosovo and Afghanistan, as well as the emerging security challenges from the East have revealed the need for a more adaptive and comprehensive approach by military intelligence.

Admittedly, reforms within military intelligence agencies are conditioned by budgetary constraints, limited human resources, legal issues and internal resistance to change. The increasingly complex nature of risks and threats, such as COVID-19, the re-emergence of ISIS, cyber-attacks or the return of former fighters from Syria and Iraq to their home states, increases the workload for military intelligence. As a result, they should be adequately resourced, staffed with professionals from diverse backgrounds, and remain adaptive. It is necessary to redefine the role of a military intelligence officer as someone capable of navigating complex environments and effectively supporting decision makers. The ability of military intelligence to process large amounts of information remains questionable, and therefore the use of modern technologies (such as blockchain) should be further explored. Alternatively, the fusion of military and civilian services should also be explored. While it is uncommon to merge civilian and military intelligence services, the contemporary dynamic security environment and the growing need to cooperate and share capacities could be argued to favor the fusion of civilian and military intelligence functions (not structures). However, while military intelligence agencies apply similar measures and methods, their consumers and target areas are different. Although NATO merged both military and civilian intelligence pillars, providing intelligence support to the North Atlantic Council and the Military Committee, this was in the context of a supra-national military alliance: the question remains whether such a merger would be appropriate on the national level, given the radically different functions and working cultures of each respective agency.

Chapter 2. Parliamentary Oversight of Military Intelligence

Dr Teodora Fuior, DCAF — Geneva Centre for Security Sector Governance

1. Intelligence oversight and its challenges

Parliamentary oversight refers to the ongoing monitoring, review, evaluation and investigation of the activity of government and public agencies, including the implementation of policy, legislation and the expenditure of the state budget. Parliamentary oversight is one of the most important manifestations of the separations of powers in a democracy.

Intelligence oversight is the newest and most challenging area of parliamentary work. National security in general and intelligence in particular, have long been perceived as the exclusive area of competency for the executive power, with legislative and judiciary bodies deferring from interference. Only in the 90s, after the end of the Cold War, has parliamentary oversight of intelligence become a norm and a prerequisite of democracy. Parliamentary oversight of intelligence is driven by three main objectives:

- To establish mechanisms for preventing political abuse and misuse of intelligence services while allowing for effective executive governance of the services.
- To uphold the rule of law by ensuring that intelligence services policies and practices are lawful and respect the values of the democratic society they serve, including human rights.
- To ensure that the use of public money is effective and efficient, according to the allocation approved by parliament within the state budget law.

The organizational complexity of the intelligence community is a first challenge for parliamentary oversight. Intelligence functions are diverse, and they are assigned to autonomous agencies and/or to ministerial departments. There are about three times more intelligence services than the number of states.⁵³ Put very simply, we can say that, in most countries, we have three types of intelligence:

- Domestic intelligence service: collecting information on the territory of the country in order to deter threats to national security (primarily a defensive mission).
- Foreign intelligence service: collecting information originating abroad and warning on impending external threats (offensive mission);
- Military intelligence service: generating intelligence relevant for defence planning. Their mission encompasses the protection of armed forces personnel, bases, capabilities and defence industry, and the support of military operations (state of preparedness, armament, deployment terrain and environment). They are often a part of the armed forces or the Ministry of Defence, and their mandates are more limited than those of the domestic and foreign (civilian) services, operating mainly at armed forces tactical and operational levels.

⁵³ For an overview of intelligence services in the 28 EU Member States see: Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update. EU Agency for Human Rights (FRA) 2017, pp. 157-161, available at: <https://fra.europa.eu/en/publication/2017/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies-eu>.

A few other agencies or departments may have intelligence functions, focusing on criminal intelligence (producing intelligence on organized crime, corruption and criminal activities to aid in law enforcement), signals intelligence, counterterrorism, drug trafficking, cyber defence, protection of dignitaries, financial intelligence, etc.

In practice, the line separating the mandates of different intelligence services is increasingly blurred. Their functions may intersect, overlap or merge. The common denominator for them all is the secrecy surrounding their operations and the use of special powers that are invasive of human rights, especially the right to privacy. Interception of communications, secret surveillance, intrusion into property, hacking, the use of undercover agents and false legal entities are just a few examples of special intrusive powers intelligence services are authorized to use.

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

Secrecy: Management, control and oversight of a large governmental bureaucracy is more complex when there is a need for secrecy. Intelligence professionals commonly have discretionary authority to make independent decisions during their work. Effective oversight of clandestine operations and discretionary decisions is difficult, as it requires expertise, access to information, effort and time. Independent but complementary oversight institutions with clear mandates for access to classified information can help overcome this challenge.

Insufficient political will: Due to the level of secrecy in intelligence services, many aspects related to intelligence oversight cannot be publicly discussed, therefore are not necessarily useful for winning citizens' attention and votes. Elected representatives may lack incentives to invest their time in intelligence oversight.

Exaggerated threat perceptions: Perceived threats to national security can be used to justify actions that may be disproportionate to the threat and harmful to the principles of democratic governance, human rights and the rule of law. A high level of professionalism, political independence and effective oversight are necessary to ensure that intelligence analysis does not over- or under-estimate the severity of a threat to national security.

Increased international scope of intelligence work: The secret nature of intelligence work applies in particular to international cooperation, which is often beyond the reach of national oversight bodies who are contained to national jurisdiction. Questions raised regarding recent practices of signals intelligence exchange and the treatment of terrorism suspects have shown that international intelligence cooperation is a high-risk area of state activity and triggered the launch of inquiries in the European Parliament and a number of countries, like Germany, Belgium, UK or Netherlands. Defining the scope and nature of international cooperation can prevent abuses and strengthen the credibility of national intelligence services.⁵⁴

Rapid developing technology: Technologies used in intelligence work advance much faster than the capacity of oversight bodies to adapt their legal mandates and expertise, creating gaps in accountability. Technical experts are essential to provide oversight authorities with key information, and parliaments need to ensure that legal framework is frequently adapted to technological developments.

⁵⁴ For a review of challenges brought by international cooperation and good practices in their oversight see: H. Born, I. Leigh, A. Wills, 'Making International Intelligence Cooperation Accountable'. DCAF and EOS, 2015, available at: <https://www.dcaf.ch/making-international-intelligence-cooperation-accountable>.

Besides the significant number of difficulties common to intelligence oversight efforts in most parliaments, ensuring accountability for military intelligences brings a few supplementary and specific challenges.

First, the regulatory base for military intelligence is less developed and/or less publicly available than for other intelligence services. International human rights standards and the rule of law require that intelligence service mandates and powers are defined in legislation. The law must be clear, foreseeable and accessible. The domestic and foreign intelligence services are most often autonomous state bodies whose functioning complies to a statutory law which clearly describes their mission, organization, powers, and restrictions in the use of special powers. Safeguards against arbitrary action are usually well grounded in these statutory laws to counterbalance secrecy and guarantee against discretionary power and lack of accountability.

In contrast with autonomous intelligence services, military intelligence is an organizational unit within the armed forces or the Ministry of Defence (or is composed of several units within both the armed forces and the Ministry of Defence), and they do not have their own statutory law.⁵⁵ Their functioning is regulated by a few articles in the law on defence,⁵⁶ and further on detailed in secondary regulation such as decrees, ministerial orders or instructions – which are not made available to the public.

This is, from the start, a weak foundation for oversight, making the accountability of military intelligence more problematic than the accountability of intelligence in general.

Comparative literature on military intelligence is not yet developed. We have seen in the last decade an increased focus of research on the oversight of domestic intelligence services and their surveillance practices. The number of reports, guidelines, manuals and academic papers on intelligence oversight has become abundant.⁵⁷ However, foreign intelligence services, and especially military intelligence remains in the shadows, with no major publication focusing on the subject. Scarce resources on the topic make it difficult for members of parliament and their staffers to build up a solid understanding of military intelligence issues. In the absence of independent analysis of military intelligence, parliament is completely dependent on the information provided by the defence establishment itself. Such a monopoly on information and expertise is not conducive to effective oversight.

Military intelligence has been relatively neglected by democratic scrutiny. The contrast with domestic intelligence services is again, blatant. At least in large parts of South-eastern and Eastern Europe, domestic intelligence services have been under a lot of scrutiny because of their support to previous communist and authoritarian regimes; regarded by the public with suspicion of being under pressure to reform and modernize. Military intelligence has benefited in many countries from the traditional public trust enjoyed by armed forces, and by high levels of support for national soldiers deployed on foreign soil in peace support or anti-terrorist operations. Consequently, while domestic intelligence services have increased dramatically their transparency to the public and have engaged in smart public communica-

⁵⁵ There are exceptions, such as Poland, where the two military intelligence agencies (SWW foreign, and SKW counterintelligence) are autonomous organizations with their own statutory law: Military Counterintelligence Service and Military Intelligence Service Act of 9th of June 2006; both services report to the Ministry of Defence.

⁵⁶ Here we use the law on defence as a generic name for the law regulating the organization and function of the Ministry of Defense and its subordinate units.

⁵⁷ See for example: A. Wills, M. Vermeulen, 'Parliamentary Oversight of Security and Intelligence Agencies in the European Union', European Parliament, Brussels, 2011, available at: https://www.dcaf.ch/sites/default/files/publications/documents/study_en.pdf See also the publications of the European Intelligence Oversight Network: <https://www.stiftung-nv.de/en/publications>.

tion campaigns, military intelligence remains in the shadows. Oversight has been minimal and formal, scrutiny arising only if and when parliaments discuss national participation in military operations abroad.

Democratic governments today accept that all state activities should be open for scrutiny and investigation by parliament. Military intelligence should not be an exception from accountability. We will analyse further what levels of action and what oversight tools are available for more effective oversight of military intelligence.

2. Levels of action in parliamentary oversight

Parliamentary oversight begins with the legislative authority to make laws and to approve government policies and continue with the regular, sustained scrutiny of how these are put into practice. By monitoring how laws and policies are implemented, members of parliament identify and correct eventual imperfections of legislation, bad administration, abuses and corruption.

Parliamentary oversight is a function of the whole parliament. There are however three complementary levels of parliamentary oversight, as detailed in Box 2: plenary sessions, committees, and individual actions undertaken by members of parliament.

Box 2. What are the levels of action in parliamentary oversight?	
Plenary session	<ul style="list-style-type: none"> Endorse security and defence policy/strategy and government 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	<ul style="list-style-type: none"> Issue reports and formal opinions on draft legislation Conduct hearings, visits, and inspections in the field Undertake inquiries (most often only after plenary approval) Investigate citizen complaints Issue oversight reports which instigate debate in the plenary Issue recommendations for overseen institutions Provide an opinion on candidates for ministerial position In some countries they may hear and provide an opinion on candidates for intelligence directors, flag officers and other high-level positions
Members of Parliament, individually	<ul style="list-style-type: none"> Propose new bills or 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 parliament activity and the focus of media attention. It represents the locus of parliamentary authority and influence on future policy formulation. All parliamentary acts and decisions with mandatory content for other entities in the state are debated and voted upon in the plenary. The Parliament is where laws are enacted, political declarations are heard, and the government's actions are evaluated.

In plenary debate, Parliaments sometimes formally approve government policy in the field of security. Strategic documents like Government Program,⁵⁸ National Security Strategy, Defence Review or White Paper for Defence shape national security policy on a long term. On the basis of a threat assessment, such documents determine the national security interests and define the priority tasks for security sector agencies. They may indicate the level

⁵⁸ The Government Program's approval in parliament is characteristic for parliamentary systems.

of defence spending,⁵⁹ the maximum number of personnel employed in security forces, the necessity for arms acquisition, and the levels of national participation in military and civilian peace support operations. Even if not specifically mentioned, these programmatic documents create the general framework for the functioning of military intelligence, and they may establish the role of different intelligence agencies and functions within the security sector.

Oversight is, however, more efficiently and visibly developed at committee level. A well institutionalized structure of standing committees, which parallels the structure of the government, is essential for the effectiveness of parliament. Strong committees develop an independent ethos, a capacity for independent, unbiased thought and action. They are the main tool for parliamentary influence in the policy-making process and for overseeing the executive.

Committees advise the plenary on all the legislation and parliamentary decisions to be taken in their field of activity. Their reports offer the starting point for all the plenary debates on legislation and are the primary vehicle for formulating recommendations to the government. Committees pursue the accountability of executive agencies (including intelligence services and departments with intelligence functions) from two main points of view:

- Administrative - investigating their policies and actions to make sure that they respect the rule of law and the rights of the population, and to avoid defective administration, waste of public resources and government corruption.
- Political - evaluating the political choices of the executive, their consistency with national interests and the program of the government, and their implementation and consequences.

3. Committees mandated to oversee military intelligence

Being the newest area of parliamentary oversight, and dealing with a complex, secretive and very country specific areas, committees responsible for intelligence oversight are diversely organized and empowered. In a comparative analysis of parliaments around Europe, no other field of parliamentary oversight is so differently organized.

Essentially, there are three approaches in setting up intelligence oversight, evolving towards increased specialization and organisational complexity:

- Defence and security committees;
- Intelligence oversight committees;
- Expert bodies for intelligence oversight.

The first two types of parliamentary committees currently convene in all parliaments of European Union member states. The expert bodies for intelligence oversight typically function outside parliament: their members are not MPs, but they are appointed by and report to the parliament. We will further explore the characteristics of these three types of intelligence oversight bodies and their comparative advantages.

⁵⁹ Usually as a percentage of Gross Domestic Product.

3.1 Defence and Security Committees

In some countries, a parliamentary committee with a wide mandate deals with legislation and oversight for the whole security sector, including Ministry of Defence, Ministry of Interior - including all of the military and law enforcement services administered by these two ministries - plus a number of other security institutions such as intelligence services and ministerial departments with intelligence activity. A decade or two ago, in many consolidated democracies and in most transitioning countries, the defence and security committee was the sole committee dealing with all security and intelligence issues. Today, this is still the case for some small countries, with a relatively small security sector, such as Albania, Montenegro and Moldova.

Given the large number of institutions and issues placed under their competency (for example, in many countries the security sector is one of the biggest employers in the economy, and receives a very large portion of the state budget), defence and security committees may only provide perfunctory oversight of intelligence institutions. More typically, they handle numerous other issues that are more important for the public and often lack the time, resources, access to classified information, and/or knowledge to focus on intelligence.

Sometimes committees with a wide mandate organize themselves in sub-committees, which focus on a specific institution or group of issues. The practice shows that sub-committees can bring benefits, allowing a small group of committee members to monitor and evaluate a particular issue and present informed reports and evaluations to the committee. However, sub-committees see their legitimacy and capacity of action minimized by a usually very small size and lack of incentives for continued and structured action.

Dealing with a wide and complex mandate can also come with advantages. Elected members and staff supporting defence and security committees develop a comprehensive understanding of the security sector and integrate legislative and oversight processes well. This is particularly important in the case of military intelligence, which is usually completely integrated organizationally in the Ministry of Defence and/or the armed forces. The defence and security committee gets an inclusive, in-depth understanding of the defence establishment which should facilitate military intelligence oversight.

Besides security and defence committees, other parliamentary committees might be competent to oversee some aspects of intelligence agency work (justice, human rights, law enforcement etc.), or might review aspects of intelligence agency work on an ad hoc basis. In addition, committees responsible for budgets and public accounts are competent to oversee the finances of each ministry and each autonomous intelligence service.

3.2 Intelligence oversight committees

A large majority of European parliaments have set up, in addition to defence and security committees, standing committees dealing exclusively with the oversight of intelligence. Sometimes military intelligence becomes part of the oversight mandate of these committees, but often it remains in the competency of the defence and security committee along with the other components of the defence establishment.

Comparing defence and security with intelligence oversight committees, intelligence oversight typically has a more narrow and focused oversight mandate. Often their responsibilities in the legislative process are limited, with the defence and security committee remaining responsible for advising the plenary on intelligence-related legislation.

The obvious advantage of a narrow mandate is the accelerated development of committee expertise: elected members and staff make the most efficient use of time and resources focusing on a small number of intelligence agencies and on oversight activities only.

Intelligence oversight committees are often joint committees, drawing members from both houses of bicameral parliaments (Romania, Bosnia and Herzegovina), in order to give them increased representativity and democratic legitimacy. Opposition is always represented, and given access to agenda setting and decision making, often having a predominant role in the committee, holding the chairmanship (Italy, Bosnia and Herzegovina, Serbia), or even the majority of committee members (Slovenia).

Further on, there are different ways of defining the mandate of an intelligence oversight committee:

- In the functional approach, one parliamentary committee is responsible for scrutinizing all intelligence agencies, or all specific intelligence functions regardless of which public bodies perform them. This avoids the risk that certain issues fall between the purviews of two or more committees. In addition to intelligence oversight committees, some parliaments have set up committees that focus exclusively on the use of intrusive powers for information collection, such as North Macedonia and Bulgaria with the committee for the oversight of communications interception, or Germany with the G10 (extra-parliamentary) committee. In countries where the mandate of intelligence oversight committees follows a functional approach, they usually have a mandate for military intelligence as well.
- In the institutional approach, committees are set up for the oversight of specific intelligence services (which are usually mentioned in the name of the committee). This is the case of intelligence oversight committees in the parliaments of Romania, Czech Republic, North Macedonia or Slovakia. This allows overseers to specialize in the work of a particular agency. Defence and security committees remain responsible for the oversight of other small services or ministerial departments with intelligence functions, including military intelligence. However, oversight may become fragmented if too many committees are involved.

Intelligence oversight committees might have a stronger legal base than other committees of the parliament; their functioning being based on a special law for parliamentary oversight of intelligence (Germany, Slovenia, Spain, Italy) on parliamentary decisions describing their mandate and powers (Romania, Poland), or on detailed parliamentary rules of procedure (Netherlands). In some cases their creation may even be grounded in the constitution (Germany). Unlike other parliamentary committees, intelligence oversight committees are sometimes requested by law to adopt their own Rules of Procedure (North Macedonia, Romania).

	Defence and security committee	Intelligence oversight committee	Expert body (extra-parliamentary) for intelligence oversight
Who is responsible for military intelligence oversight?	Albania, Romania, Bosnia and Herzegovina, North Macedonia, Montenegro, Hungary, Lithuania, Latvia, France, Spain	US, Finland, Denmark, Poland, Czech Republic	Norway (EOS); Belgium (Committee I); Netherlands (Review Committee on Intelligence and Security Services); Portugal (Council for the Oversight of the Intelligence System); Switzerland (independent supervisory authority for intelligence activities); Finland (intelligence oversight ombudsman)
Characteristics			
Members	Proportional representation of major parliamentary 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 appointment.	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. Parliament rules of procedure	Strong. Special law or parliament decision, own rules of procedure	Special law
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	General: Thorough understanding of security sector	Focused: In-depth understanding of intelligence sector	Focused: Strong secretariat and expert support (13 staff 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 very informative reports on intel.
Disadvantages	Lack of time and interest to focus on military 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

Besides benefiting of a clear legal base and a sustained focus on a narrow mandate, which are conducive to faster development of expertise and effective oversight procedures, intelligence oversight committees may count a few other advantages.

One of the most important advantages is democratic legitimacy. Intelligence oversight committees are composed of elected representatives, and opposition has, usually, a clear and important role in decision making. Oversight involving a number of political parties can help to ensure that intelligence agencies serve the interests of society as a whole rather than an incumbent government. The involvement of opposition parties in oversight committees can serve as a valuable counterweight to a governing party's position in the intelligence domain.

In terms of impact on overseen institutions, the findings and recommendations of intelligence oversight committees must be acted upon by the executive and intelligence agencies. Parliaments have a number of tools to ensure such influence: budgetary appropriation; discharge of powers in the cases of some officials; political pressure; amending legislation and so on.

There are, however, a few significant challenges and drawbacks in the work of such committees.

The first, is the politicization of oversight. Partisan aims are often not necessarily compatible with the demands of conducting effective, independent oversight, which requires parliamentary committees to scrutinize the work of the executive and its agencies according to objective, legally defined criteria. For example, MPs that are part of the governing party may not be inclined to shed light on issues or events that are likely to be damaging to the government. By contrast, MPs from opposition parties sometimes seek to use their position on an oversight committee for political gain, e.g., by using the powers of their committee position to compel testimony from government ministers on issues wherein they hope to derive a partisan advantage. The instability of parliamentary politics is another drawback to parliamentary oversight of intelligence agencies; notably, some 'maverick' parties might consider leaking information for political or other gain.

Second, parliamentary committees (defence and security, and intelligence oversight as well) rarely dispose of sufficient expertise and time for effective oversight. Parliamentarians are often members of several committees; they have to spend time in plenary debates and to engage with their constituents. These competing responsibilities reduce the time available for detailed oversight of intelligence agencies. Time constraints on oversight are further increased when members of specialized parliamentary oversight bodies are also party/group leaders or spokespersons within a chamber. An inevitable consequence of the numerous demands on MPs' time is that parliamentary oversight committees do not meet very often. For example, the German Bundestag's Parliamentary Control Panel - one of the strongest examples of a specialized parliamentary oversight committee - meets only once per month. MPs often lack the expertise that is necessary to understand intelligence agencies, and lack the time to learn and develop this expertise. This problem is further compounded by the relatively short tenures of committee membership due to frequent elections or the desire of party leaderships to rotate their members between committees in parliament.

Box 3. Examples of intelligence oversight committee competent over military intelligence

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

Oversees 17 agencies: controls the entire intelligence community (functional approach) including military intelligence

Established in 1976 (Senate) and 1977 (House of Representatives), after a one-year parliamentary investigation of abuses by CIA, NSA, FBI (Church Committee)

Members appointed by House (22) and Senate (15) 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 authorizes use of secret surveillance

Intelligence Oversight Act 1980 requires prior notice of Congress for all important operations: ensured by the Gang of Eight: a bi-partisan group of leaders in Congress who are briefed on top classified intelligence operations⁶⁰

Committees meet roughly twice a week for 1.5 to 2 hours, generally in closed session.

Have their own rules of procedure⁶¹

Relevant subcommittees: United States House Intelligence Subcommittee on Defence Intelligence and Warfighter Support

German Parliamentary Control Panel (PKG)

Oversees six agencies, including the Military Counter-Intelligence Service; 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.

⁶⁰ 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 criticize later if something goes wrong.

⁶¹ For more information, see: <https://www.intelligence.senate.gov/about/rules-procedure>; <https://docs.house.gov/meetings/IG/IG00/CPRT-116-HPRT-IG00-CommitteeRules.pdf>.

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

3.3 Expert intelligence oversight bodies

In addition to parliamentary committees, an increasing number of states are establishing expert intelligence oversight bodies, external to parliament. Belgium, Denmark, Germany, Greece, Norway, Netherlands, Sweden, Croatia, North Macedonia, Switzerland, Portugal and Finland provide some examples.

The members of these bodies are senior public figures, prominent members of civil society, current and former members of the judiciary or former politicians, usually appointed by parliament and reporting to parliament and/or the executive. Expert bodies are generally independent from parliament and the executive, organizationally and operationally. They act autonomously in decision-making processes, including deciding which matters to investigate and report on, and often have their own budgets approved by parliament. They have strong secretariat and expert support staff, employed on a permanent basis, and therefore are able to conduct oversight on an ongoing and full-time basis.

Expert bodies are most often mandated to oversee the legality of the work of intelligence services and the respect of human rights, but their mandates may also include monitoring the effectiveness of operations, administrative practices, or the use of intrusive methods for information collection. Most often they complement the work of parliamentary committees (i.e., defence and security committees), but in some cases parliaments completely outsource oversight to a specialized autonomous body and do not have any specific parliamentary committee for the oversight of intelligence agencies

The advantages of this model are the inverse of drawbacks associated with parliamentary oversight committees:

- They are normally professional bodies whose members do not have other occupations. This means that they have more time to dedicate to oversight.
- Members of non-parliamentary oversight bodies usually have a much longer tenure of membership which gives them the opportunity to develop expertise over time. They also have fixed tenures of office, which means that their position is not normally dependent upon changes in government or changes in the balance of power in parliament.
- Oversight by non-parliamentary bodies is continuous: it does not halt when parliament is in recess or dissolve for elections.
- Members are often selected based on their qualifications to ensure the requisite expertise to conduct effective oversight.
- They are generally regarded as being more independent than members of parliamentary bodies because they do not hold political office and/or operate in an environment where oversight can be used for political gain. There are often strict safeguards to ensure that members do not engage in any other activities which could compromise their position. For example, they may be barred from holding elected office and/or having private business interests for the duration of their membership.

The most significant drawback to non-parliamentary oversight bodies is that they may be perceived to lack democratic legitimacy. Unlike members of parliamentary oversight committees, members are not directly elected. Consequently, overseers are removed from the public on whose behalf they conduct oversight.

Box 4. Examples of extra-parliamentary oversight bodies competent over military intelligence

Norway Parliament Intelligence Oversight Committee (EOS)

- Oversees all Norwegian entities that engage in intelligence, surveillance and security activities, including Defence 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 hold a maximum of ten years. It should be avoided that more than four members are replaced at the same time. Persons 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 monitoring and gathering of information and processing of personal data. No legislative power, no budget competency
- Powers: Extensive right of access to information and premises (about 60 inspections a year -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 to review use of extraordinary powers. Decides if surveillance measures are legal and necessary. Can refuse to approve operation.

Finland Intelligence Ombudsman

Autonomous, independent authority established in 2019; appointed by Government for a five-year term, with a mandate to:

- Supervise the legality of civilian and military intelligence activities and gathering methods
- Supervise the respect for human rights in intelligence activities
- Promote legal protection and best practices in intelligence activities
- Assess the functionality of legislation and make legislative development proposals
- Work cooperatively with the Intelligence Oversight Committee of the Parliament

4. Tools for parliamentary oversight

Despite their different organization, composition, mandate and powers, the committees responsible for military intelligence oversight are using the same oversight tools whose foundation is parliament's legal power to get information from the executive, and consequently to demand documents and reports or to summon executive officials to committee meetings and demand that they explain and justify their actions.

Committee oversight activities are independent from the plenary or from the legislative schedule. They settle their own program and oversight agenda, they decide whom they invite to hearings or to committee meetings, which may be open or closed to the public, depending on the decision of members.

There are two distinct yet complementary oversight strategies:

Proactive: Committees engage in “police patrol” activities, which are regular and planned (requiring discussions with the overseen agency) and include regular meetings to discuss legislation or recent policy developments, regular activity reports submitted to the committee, field visits to headquarters or regional premises and offices, etc. The committee's Annual Work Plan - disseminated to security institutions and interested partners - builds trust and offer transparency in relationship with the executive and the public. It also provides stability and gives committee members the opportunity to plan their activities for the year ahead.

Reactive: when committees act only after a “fire alarm” sounds, and they organize hearings or inquiries to investigate problems highlighted in parliamentary debates, media, or complaints received. Committees have the authority to summon ministers, military or civil servants, agency directors or independent experts, in order to answer the committee's questions or even testify under oath.

To achieve good results, it is important for the committee to understand and plan oversight as a process, and not as independent, isolated activities. Different oversight tools are better suited to different stages of the oversight process.

Getting information and acquiring a good understanding of the intelligence sector is achieved through reports, consultative hearings, and field visits.

Oversight hearings, field visits, and inquiries allow committee members to develop their expertise in security matters and engage in an informed dialogue with executive officials, ask clarifications and specific details, and develop their capacity for independent analysis.

Having acquired information and expertise, the committee is better equipped to assess the performance of the security sector, identify weakness and formulate solutions in the form of laws, amendments to laws or recommendations for the security sector institutions.

4.1 Reports

Reports are one of the most powerful and most frequently used oversight tools. According to the principles of the Rule of Law and separation of powers, all government departments in a democratic state are obliged to report to parliament and to the public.⁶² This is a prerequisite of democratic accountability. Reports enable parliament and other oversight bodies to analyse whether there is adherence to government policy and the legal framework, and

⁶² 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 intelligence services.

if taxpayers are receiving value for their money. Intelligence services are not excluded from this practice.⁶³

There are two categories of reports: regular activity reports proactively submitted by services to the committee/parliament, and special reports on specific topics, drafted at the request of the parliament.

Regular activity reports of ministries and intelligence and security services are the most common type of reporting and the most frequently used oversight instrument in parliamentary committees.⁶⁴ There are many examples of intelligence services that regularly (usually annually) publish activity reports providing comprehensive and useful information for oversight without compromising national security.⁶⁵ Sometimes, the text that is made publicly available does not necessarily contain all the information that was initially provided to the parliament, with some information being removed from the public version.

Regular activity reports can vary greatly in terms of length and content depending on the local custom and the legal definition of the requirements of the oversight body to whom the report is addressed. In spite of all differences, the reports generally follow a similar logic and contain information in three broad areas: the intelligence agency itself and its work (how tasks were fulfilled during the year), the threats to national and regional security (drawing on the most important findings of intelligence analyses), and oversight (how the agency engaged with oversight bodies, the general public, and how it executed its budget) provisions.

- The length can vary from 20-30 pages (in Netherlands, Czech Republic, Croatia) to a very detailed in-depth report (e.g., Australia ASIO Annual Report 2019-20: 160 pages).
- The content may cover, without divulging sensitive details: the annual objectives and priorities of the service; its assessment of major threats to security; any major reforms of intelligence policies, systems, and operations; fulfilment of the reporting and accountability functions of the service; and the response of the service to requests for information under freedom of information legislation.

The problem with military intelligence however is that being a part of Armed forces or the MoD, they have no legal obligation to prepare and submit their own report to parliament, though eventually they're referred to in reports drafted by the MoD. However, oversight committees can request special reports to compensate for the lack of regular reporting.

Special reports are a supplement to the general yearly reports, and they are requested by the oversight body on specific topics identified to be problematic or of special interest. The origin of such special requests for reports may lie in legal provisions or may be a consequence of media scandals, security incidents or targeted hearings and inquiries of oversight bodies. The special reports are usually produced by the intelligence service or department which is interpellated; sometimes they are based on research carried out by legal and in-

⁶³ H. Born, A. Wills, 'Overseeing Intelligence Services: A Toolkit', p. 57, available at: https://dcaf.ch/sites/default/files/publications/documents/Born_Wills_Intelligence_oversight_TK_EN_0.pdf.

⁶⁴ The U.S. Department of Defence Senior Intelligence Oversight Officer is reporting as designated Point of Contact within the Department of Defence to the oversight body on a quarterly basis.

⁶⁵ See for example links to recent public reports of main intelligence services from Australia, Canada, Croatia, Czech Republic, and the Netherlands at the following links - ASIO Annual Report 2019-20, available at: <https://www.asio.gov.au/asio-report-parliament.html>; CSIS Public Report 2019, available at: <https://www.canada.ca/en/security-intelligence-service/corporate/publications/2019-public-report>; available at: [html](https://www.soa.hr/hr/dokumenti/javni-dokumenti-soa-e/); Security-Intelligence Agency 2019 <https://www.soa.hr/hr/dokumenti/javni-dokumenti-soa-e/>; Security Information Service 2018, available at: <https://www.bis.cz/annual-reports/>; AIVD Annual Report 2019, available at: <https://english.aivd.nl/publications/annual-report/2020/09/03/aivd-annual-report-2019>.

investigative staff into the files of the service, with an oversight mandate given by the overseeing body/committee.

Special reports require the demanding committee to ask accurate and target-oriented questions. The reporting requirements must be exhaustive enough to answer the question to be answered by the report, but not be excessive in order to avoid being buried in a large amount of irrelevant information. In that sense, too much information can be just as limiting to effective oversight as too little information.

Box 5. What kind of special reports may 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 additionally 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, and data 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 may be prosecuted by the Attorney General.

Based on focused inquiries:

- 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, as in most cases, to the Prime Minister (in classified form) and to Parliament (with sensitive material redacted).⁶⁶

A condition for making oversight-based on reports effective is for the parliament to set clear and strict timelines for the submission of reports, and their debate in the committee (or plenary if that is the case).

Reports coming from government departments, and especially from intelligence agencies are written with an eye to 'public relations' and therefore are unlikely to present the whole

⁶⁶ Intelligence and Security Committee of Parliament, 'UK Lethal Drone Strikes in Syria', 26 April 2017, p.1 – 4, available at: <http://isc.independent.gov.uk/news-archive/26april2017>.

picture. They are important because they provide a starting point for overseers to develop their questions and investigative strategies, while using other, more elaborated tools of oversight.

4.2 Hearings

Hearings can be the most efficient instrument of oversight, if properly used by the parliament. The hearings agenda of the parliament reflects the most important issues of the day and what occupies parliament attention. Based on the constitutional right of parliament to get information from the executive, standing committees have the right to demand the attendance of executive officials to their meetings, as often as they want, in order to provide information supplementary to regular government reports. Some parliaments make the distinction (in law, procedure or practice) between consultative hearings and oversight hearings.

Consultative hearings are often organised on policy or legislative matters, for consultation with government officials, independent experts and/or other parties concerned. Consultative hearings are allowing parliament to better fulfil their legislative function; they allow committees to gather information to review past legislation, to consider pending legislation or to explore and better understand issues that may require legislation in the future. The detailed, first-hand information obtained during the hearing should enable the committee to make better informed analyses and decisions on the matter.

- Sometimes, consultative hearings are called in an informal manner, and no verbatim record of the meetings is made.
- Often public, consultative hearings improve the transparency of the committee and inform the public on certain policy issues.

Oversight hearings aim to obtain evidence or in-depth explanation on a specific matter. They are an effective tool for keeping the executive (including security institutions) accountable, and even for uncovering possible wrongdoings, misadministration, corruption or abuse of power and determining if there are grounds for impeaching a government official. Government officials are invited to provide information and respond to questions in their area of competency. In most countries, laws and rules of procedure stipulate the obligation of the summoned officials to appear in front of the committee and provide the requested documents and information (sometimes documents may be sent before the hearing takes place). Other experts from civil society, academia or independent institutions can be invited to provide evidence. Oversight hearings usually conclude with a report which might include recommendations for the government or the intelligence service.

- 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 to the press or 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 only during a parliamentary inquiry.

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

1. A first factor is the independence of the committee in deciding on its hearing agenda:
 - The decision to hold a hearing is generally taken by a simple majority of committee members, without any requirement for approval of the parliament plenary or its governing bodies.
 - Committees also have extended powers in establishing the topic of a hearing and the executive officials invited to provide information.
 - The decision if the hearing will be public or in camera is usually made by a majority of members.
2. A second factor is the Committee's power of investigation:
 - In some parliaments the committee's power to summon persons into hearings is limited to ministers and government officials, but in others, committees may request attendance of experts outside the government in order to obtain a different perspective on the issues under discussion and break the monopoly usually held by government on security and intelligence information. A wide range of people should be invited to provide their views and expertise, orally and/or in writing, including government officials and ministers, interest groups (professional associations, unions), academics, specialists, NGOs, members of the public, women's organisations etc.
 - Committee members should coordinate, thoroughly prepare and plan before the hearing, so that their questions are pertinent, cover different areas and do not repeat each other.
3. A third factor is the Committee's ability to ensure a follow-up of the hearing:
 - A broad engagement of officials and expert input allow the committee to elaborate sound, evidence-based evaluations and pertinent recommendations.
 - If hearings do not provide the committee with satisfactory evidence and information on the subject of their investigation, or if they indicate that a matter needs further, more in-depth investigation, the committee may propose the plenary to set up an inquiry committee, with a specific mandate. In rare cases, permanent committees can initiate inquiries themselves, without the support and the vote of the plenary (Germany, Montenegro). Inquiry committees have subpoena powers, in most parliaments.
 - Public hearings give visibility to the work of parliament, helping it demonstrate its relevance and legitimacy to the general public. They help the public understand what the parliament does and what its effectiveness is in pursuing government accountability; they may also add public pressure towards the implementation of parliament recommendations.

The parliamentary intelligence oversight committee of the German Parliament (PKGr) has started organizing 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 major trends and incidents of importance in their area of activity.⁶⁷

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 the German Military Intelligence Agency (MAD) by the Minister of Defence. The elite KSK (Special Forces Command) was also partially disbanded in June 2020, as 20 of its members were suspected of right-wing extremism.

⁶⁷ Gestiegene Gewaltbereitschaft in allen Bereichen des Extremismus. Bundestag.de, available at: <https://www.bundestag.de/dokumente/textarchiv/2020/kw27-pa-parlamentarisches-kontrollgremium-bnd-699648>.

4.3 Field visits

Field visits are powerful tools of oversight, as they offer members of parliament the opportunity to access first-hand information about the work of intelligence, engage with a larger number of military and civilian personnel than in parliamentary hearings, as well as to check premises, technical equipment, and files. For MPs, field visits are a great opportunity to understand the realities of the institutions they oversee, while for the overseen, they offer a chance to explain the challenges of their work, to build trust with the oversight body, and to advocate for budgetary and legislative support from parliament. Field visits can also be organised abroad, where military troops are deployed in humanitarian or peace-keeping operations.⁶⁸

Unlike hearings, which are based on interaction and dialogue with officials who come in the premises of the committee, in a field visit the committee goes out on an explorative mission to territories it doesn't fully know, understand or control. The risk for losing the focus and getting derailed from its oversight objective is high. Therefore, the need for relying on expert staff support is more relevant on a field visit than with 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 the 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. Each stage of this process is different - depending if the visit is organized as a proactive oversight activity (announced well in advance, eventually included in the annual programme of the committee), or if it is a reactive visit to carry out an investigation of some specific allegation or incident. In intelligence oversight especially, even if inspection visits may be called "unannounced" by law and procedure, the practice of most parliaments shows that they are always announced, 24 to 48 hours before.

Box 6. How to develop a committee's experience and practice in organising field visits

Ideally the Committee Rules of Procedure describe with detail and 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 well in advance, along with general topics and objectives such as a better understanding of the intelligence organisation, 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 start taking place. Foresee that eventually, even in an "announced visit period", visits can take place after 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

⁶⁸ Visits to the theatre of operations where national soldiers are deployed are undertaken by defence and security committees, with the support of the Ministry of Defence.

on 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 preparation 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, but is also a missed opportunity to establish and improve good oversight.

4.4 Inquiries

Inquiries are a very strong oversight instrument and have an important potential to reveal facts veiled 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-defining the topic, the scope and the timeline of the inquiry.

A parliamentary inquiry requires special powers of investigation, also called subpoena powers. This means that the rules of criminal procedure shall apply *mutatis mutandis* to 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, but also 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, similar to 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 must provide clear instructions about the conditions in which an inquiry may be initiated, allowing equitable participation of opposition and minority groups in the decision about the organization and the mandate of an inquiry. Very few standing committees have the power to lead inquiries and when they do, they must obtain permission and a mandate from the plenary (exceptions are met in Germany, Belgium, the Netherlands, Canada, and Montenegro).

Most often, parliamentary inquiries are led by cross-party ad-hoc 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 of concern, but within a reasonable time frame so that lessons can be learned promptly. They are given a certain deadline to conduct their investigations. After submitting their final report to the parliament, the committee of inquiry is dissolved.

Despite the similarities between their proceedings and those of judicial procedures, inquiry committees should not be confused with criminal investigations as 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 due care.

The Venice Commission has formulated recommendations for instances in which an inquiry committee discovers elements that suggest a criminal offence might have been committed:

1. Inform the public prosecutor and hand over relevant information and documentation to the prosecuting authorities to the extent that it is allowed to do so under national law.
2. The discovery of possible criminal offences should not in itself stop an otherwise legitimate parliamentary process of inquiry. The inquiry should proceed, and the committee should continue to examine the case and make its own (political) assessments. In particular, it should be able to continue to examine the facts of the case, even if these facts may also be of relevance to criminal proceedings.
3. Establish proper procedures for cooperation and exchange of information and evidence between the committee and the public prosecutor, while respecting the differences between the two processes as well as the procedural rights of the person suspected of having committed a criminal offence and other persons appearing in front of the committee.
4. Properly take into account the pending criminal investigations or proceedings and exercise caution so as not to make assessments or statements on the issue of guilt, or to infringe upon the principle of assumed innocence in other ways. The committee should take great care to ensure that its inquiries do not obstruct or in any other way unduly interfere with the criminal investigations or proceedings.
5. When formulating its report, the parliamentary committee should take great care not to make any assessments of a criminal legal nature or assign criminal responsibility to any of the persons concerned. It should, however, remain free to describe and analyse all facts of the case and to assess these from a political perspective.
6. The fact that persons who don't hold public powers are involved should not restrain a parliamentary committee from enquiring into the behaviour of such persons to the effect that it is of relevance. Therefore, if a public scandal is being scrutinized, the fact that a person is a private person and does not occupy any public role should not exempt them from being summoned to appear in front of a Commission.

Box 7. What special investigation powers may inquiry committees have?

In the German Bundestag,⁶⁹ the Defence Committee has an outstanding position because its formation is the only committee which may declare itself to be a committee of inquiry. In the case of all other committees, the Parliament must take a decision to this effect. A committee of inquiry is the 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 EUR can be placed on absent witnesses or on those who refuse to surrender an item required by the inquiry committee as

⁶⁹ Basic Law, Art 45a, par 2.

evidence.⁷⁰ In instances of a repeated failure to comply, the administrative penalty may be levied again.

A witness who refuses to testify can be obligated 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.⁷¹ The judge can also order a search for the seizure of items requested by the inquiry committee as evidence.⁷²

The federal government is required to grant the necessary authorization for the examination of office holders.⁷³

In France, the refusal to appear in front of an inquiry committee and to respond to its questions can be punishable by 2 years of imprisonment and a fine of 7,500 EUR.⁷⁴

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 1 year of prison and \$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 prescribing fines that can go up to 2.000 Euros for employees and to 20.000 Euros for legal entities.⁷⁵

In practice, inquiries are an oversight tool that are rarely used, often as a last resort. Few parliamentary inquiries have delivered satisfactory results, at least in the areas of intelligence, defence and security. This modest record is often caused by insufficient investigative resources and skills put at the disposal of inquiry committees, very high costs, and long delays caused by the involvement of lawyers and endless disputes about access to documents. This suggests that in most countries, the information parliament gets is ultimately the information the intelligence services decide to share.

Below are a few examples of parliamentary inquiries in security and intelligence area:

- Germany's "NSA Inquiry" (Untersuchungsausschuss 'NSA') launched in the Bundestag in March 2014 was set up to investigate the extent of foreign secret services spying in Germany. The committee met 131 times over a period of three years, with 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 has transformed to investigate the legality of German intelligence governance and has identified important oversight deficits, preparing the path for major intelligence reforms.
- In France and Belgium, the respective national parliaments created a special inquiry committee after the terrorist attacks of 2015 and 2016.

⁷⁰ Law on Inquiry Committees, section 21, 27, and 29.

⁷¹ Ibid. Section 27 (2).

⁷² Ibid. Section 29 (3).

⁷³ 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.

⁷⁴ Art. 6 of the 1958 law on the functioning of Parliament.

⁷⁵ Art.22 of the Law on Parliamentary oversight of defence and security sector, adopted December 2010.

- In 2006, the Romanian Senate established an ad hoc inquiry committee that, over two years, investigated the existence of secret CIA detention sites on national territory. The report was kept entirely secret except for its conclusions, which categorically denies the possibility that secret detention facilities could be hosted on Romanian soil. The “Fava Inquiry” of the European Parliament (2007) and the ECHR case *Al Nashiri v. Romania* (2018) later raised further questions.
- In Bosnia and Herzegovina, in 2011, the Joint Committee for Defence and Security, with the approval of the National Assembly, established itself as an inquiry committee to investigate the legality of the destruction process of ammunition, mines and explosive ordinances, weapons, and military equipment led by the Defence Ministry between 2006 and 2009. All information collected was given to the public prosecutor, with a request to launch an investigation. This never happened.
- In 1994, the States General (Dutch Parliament) created a parliamentary commission of inquiry into the 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 organization of criminal investigations in the Netherlands, leading to major legislative reforms.
- The Intelligence and Security Committee of the UK Parliament, over the course of eight months, conducted an inquiry into the threat posed by Russia to the UK (cyber, disinformation, and influence), and the response of the UK government. The report was published in July 2020.⁷⁶

Inquiries receive more public attention than regular parliamentary activities. Therefore, they bring a spotlight to issues under scrutiny and shape the public agenda. Inquiries bring visibility to the work of parliament and thus may enhance public trust in this institution and build upon parliament’s credibility and legitimacy within the democratic system.

⁷⁶ Russia, Report of the Intelligence and Security Committee of Parliament, available at: <https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbnRlbnQuZ292LnVrfGlzY3xneDo1Y-2RhMGEyN2Y3NjM0OWFI>.

Conclusion

A sub-standard legal base, insufficient expertise and little public attention have deprived military intelligence oversight of effectiveness in too many countries and for too long. In most parliaments there is no routine oversight over military intelligence. This is especially true in countries without significant military participation in peacekeeping operations abroad, or in the countries where parliament doesn't have a role in the decision-making on foreign deployments. But military intelligence should neither be taken for granted nor overlooked, for their role in supporting both foreign and domestic policy is too important. Because of the complexity, political nature and the secrecy characterizing the work of military intelligence, it is paramount for the parliament to have sufficient legal powers, ability and willingness to keep this sector accountable.

Military intelligence is an overlap of two worlds – armed combat and clandestine operations. It is for this reason that the oversight of military intelligence is assigned and defined so differently from one parliament to another. Some countries run into difficulties when deciding which committee, defence or intelligence, parliamentary or non-parliamentary, is the natural go-to committee to exercise oversight over this segment of security sector. Whichever model is chosen, it comes with advantages and challenges to ponder. But the most important risk to mitigate is that among the many institutional approaches and accountability trials our societies are facing today, military intelligence sometimes escapes between the forks of oversight. A holistic and results-based approach must be taken. The important question is not what sort of and how many oversight bodies are established, or what oversight tools are more frequently used, but whether the result is effective oversight.

Chapter 3. Parliamentary Oversight of Military Intelligence Agencies: A Comparative Overview

Dr Mindia Vashakmadze

1. The role of military / defence intelligence agencies in modern democracies

There are a variety of models of military intelligence agencies in different countries which operate at the intersection of the respective Ministry of Defence and the intelligence community.⁷⁷ A main organizational feature distinguishing military intelligence from civilian intelligence services is their subordination to the defence sector and integration into the structure of the respective Ministry of Defence and/or the armed forces.⁷⁸ For instance, in line with the Estonian Defence Forces Organisation Act, “the Military Intelligence Centre is a structural unit of the Defence Forces, whose task is to execute military intelligence and coordinate the intelligence and security operations of other structural units, provide the Minister of Defence, the Commander of the Defence Forces and the Deputy Commander of the Defence Forces with intelligence and security information, and perform other functions arising from the legislation.”⁷⁹

Distinction can be made between the military intelligence components that form a part of the armed forces and the agencies that are located outside the army structure, maintain the civilian status and perform military intelligence tasks. In many cases, different types of military / defence intelligence components operate at the same time that are not subject to the same oversight regime.

The subordination of military intelligence to the command structures has been regarded as a challenge to parliamentary oversight. The Venice Commission of the Council of Europe noted in this regard: “Military agencies can be distinguished from civilian agencies. The principal mandate of the first may be confined to intelligence collection relating to military threats to the State, and the security/loyalty of the armed forces, although again the boundary line between this and the mandate of a civilian agency may be difficult to draw. Where a security agency is located organizationally within the military command structure, this can give rise to special problems of accountability”.⁸⁰

The military intelligence agencies cooperate with different security sector agencies at the domestic level and internationally alike. In particular, they provide support to the armed

⁷⁷ See, for example, on the US Defense Intelligence: ‘Defense Intelligence Agency – Strategic Approach’, September 2018, available at: https://www.dia.mil/Portals/27/Documents/About/DIA_Strategic_Approach.pdf.

⁷⁸ However, the degree of affiliation with the command structure and the integration of military intelligence services with the armed forces varies from country to country. For example, in Portugal, the Military Information and Security Centre is a part of the General Staff of the Armed Forces. Its head is a high-ranking military official. The military intelligence agency of Spain has a similar structure – The Spanish Armed Forces Intelligence Centre (CIFAS) is a part of the Armed Forces. It is a joint body of the Armed Forces on intelligence and acts as a complementary military intelligence body to the National Intelligence Centre, with which it is coordinated through the Joint Military Intelligence Plan. According to the Law 11/2002, the National Intelligence Centre is attached to the Ministry of Defence, which remains accountable to parliament for the activities of the military intelligence services.

⁷⁹ Estonian Defence Forces Organisation Act, par 22.

⁸⁰ Venice Commission, ‘Report on the Democratic Oversight of the Security Services’, CDL-AD(2007)016, par 90.

forces deployed abroad within the framework of collective peace efforts or on a bilateral basis, take part in inter-state information systems, and share intelligence with foreign defence intelligence agencies as well as with local security services and law enforcement. A closer and continued cooperation with other security agencies and law enforcement gained a significant importance in the context of modern transboundary threats. At the same time, the tasks and responsibilities of the military intelligence agencies as well as the means they use in their daily work are getting increasingly complex and intrusive. Military/defence intelligence services conduct a full range of intelligence operations including human intelligence, signals intelligence, imagery intelligence, open sources intelligence, and other varieties. A broad spectrum of tasks, increasing international cooperation and networking as well as the modes of operation of the military intelligence agencies (including the collecting and sharing personal data) raise fundamental challenges not only in terms of effective parliamentary oversight but also may create risks of disproportional and unjustified interferences with fundamental rights. As regards their working methods, military intelligence agencies use a broad spectrum of means that are equally available to civilian intelligence agencies.

The complexity and range of military intelligence operations as well as their administration and management structures should be taken into account when designing respective oversight mechanisms. Defence/military intelligence capabilities and management may be concentrated in a single agency or rather dispersed throughout the entire system of the armed forces and the defence sector. Although they are mostly placed within the purview of the respective ministry of defence and the armed forces, recent developments demonstrate that the countries are trying to ensure better coordination, effective management and oversight as well as more effective information sharing between intelligence agencies.⁸¹ To achieve this objective, new coordination structures are created, and the regulatory frameworks reshaped. For example, in Australia, it was a key recommendation from an independent Review of the Defence Intelligence Enterprise to create a new Defence Intelligence Group to place all of ADF's intelligence capabilities under a single oversight institution and "to ensure the organisation is best positioned to support Australian Defence Force."⁸² With respect to Canada, it has been noted that "the administration of defence intelligence remains challenging due its complexity and sensitivity, as well as the fact that defence intelligence expertise and resources are widely dispersed across DND organizations and CAF command."⁸³ The 2018 Annual Report emphasized the need for statutory regulation of defence intelligence and indicated that this would be conducive to effective protection of fundamental rights.

Moreover, effective organisation and administration of military intelligence having a sound legal footing is equally conducive to democratic accountability.

Due to the emergence of new perceptions of threats, the evolving roles of the armed forces, transforming intelligence practices as well as the blurring between domestic and international security and military risks, the material and territorial scope of the activities of military intelligence agencies is expanding. This poses additional challenges to accountability. Since the military intelligence agencies are closely associated with the respective ministries

⁸¹ See, for example, Australian Defence Business Review, 'Australian Government Forms New Defence Intelligence Group', 7 December 2020, available at: <https://defense.info/defense-decisions/2020/07/australian-government-forms-new-defense-intelligence-group/>: "The Commonwealth has announced the formation of the Defence Intelligence Group (DIG) from July 1 to bring all of the ADF's intelligence capabilities under a single oversight organisation and to coordinate the introduction of new capabilities. The new group includes the Defence Intelligence Organisation (DIO), Australian Geospatial Intelligence Organisation (AGO), and other critical intelligence components from across the ADF."

⁸² Australian Government, 'Strengthening Defence Intelligence', 22 June 2020, available at: <https://australiacybersecuritymagazine.com.au/strengthening-defence-intelligence/>.

⁸³ The National Security and Intelligence Committee of Parliamentarians, 'Annual Report 2018', April 2019, par 4.3.

of defence and the armed forces, the main channel for ensuring accountability often is the political accountability of the respective Ministry of Defence to parliament. At the same time, as this comparative overview shows, it is essential to also establish specialised parliamentary and effective non-political external oversight mechanisms that are complementary to general parliamentary oversight.

2. Shaping regulatory framework for military intelligence oversight

The legislative framework should introduce and strengthen a functional separation of powers between the executive and legislative branches with respect to overseeing the activities of intelligence agencies in general, and military intelligence in particular. Additionally, it is equally crucial that the legal framework safeguards fundamental rights and guarantees a necessary degree of transparency in the domain of military intelligence. The law should reconcile effective executive authority over military intelligence with democratic accountability.

It is interesting to observe in state practice how accountability relations and processes triggered by major military intelligence shortcomings or the abuse of power by intelligence agencies shape regulatory framework in the respective country in the mid-to-long term⁸⁴ and how a newly introduced regulatory framework influences and eventually improves accountability. At least, it may create preconditions for further improvements. Several stakeholders are involved in this process.

In a democracy, parliaments play a central role in introducing and strengthening a sound regulatory framework for the activities and oversight of military intelligence agencies. The standing committees on defence also take part in this process. However, the degree of their involvement varies from case to case. In the countries under consideration, the committees fulfil a range of tasks. In particular, the committees discuss legislative proposals, draft amendments submitted by the respective government for consideration, formulate their legal position and elaborate on the political and financial aspects of the proposed legal amendments. In some cases, the committees may initiate new proposals and recommendations to change the regulatory framework.⁸⁵

The scope and specifics of parliamentary involvement depends on the respective system of government and its characteristics. At the committee level, it also depends on the scope of the mandate and the division of responsibilities in parliament. Under certain favourable circumstances, the position of a defence committee or another oversight body may play a central role in the process of adoption of a new or amended existing regulatory framework for military intelligence oversight.

Furthermore, the parliamentary inquiries and ad hoc investigations, which may uncover certain gaps in the regulatory framework, can also indirectly contribute to or even trigger a certain reshaping of the existing legal framework. The standing parliamentary committees on defence and security often do not deal with the analysis of the legislation governing military intelligence work on a permanent basis and in a systemic and comprehensive manner. Rather, these committees have oversight responsibilities and other tasks. Therefore, the non-parliamentary oversight bodies, independent review commissions or ad hoc inquiry

⁸⁴ See, for example, the Knesset website, 'Agranat Commission', available at: https://www.knesset.gov.il/lexicon/eng/agranat_eng.htm. See also U. Bar-Joseph, 'The Politicization of Intelligence: A Comparative Study', *International Journal of Intelligence and Counterintelligence*, 2013, 26:2 pp. 347-369.

⁸⁵ For example, the Lithuanian parliamentary oversight committee contributes to the improvement of the overall regulatory framework by submitting proposals concerning improvement of the legal acts related to activities of intelligence institutions and protection of human rights in the area of intelligence and counterintelligence. Survey findings from Lithuania on file with the author.

commissions may also play an important part in legal reforms related to military intelligence activities. The international practice shows that the major inquiries into intelligence activities or the proposals of the external (non-parliamentary) review bodies contributed to significant changes in the regulatory and institutional framework or at least generated a debate over the role and responsibilities of the military intelligence agencies. For example, the National Security and Intelligence Committee of Parliamentarians in Canada (NSICOP)⁸⁶, which is not a parliamentary oversight body, has recommended to the Government to “give serious consideration to providing explicit legislative authority for the conduct of defence intelligence activities.”⁸⁷ The Committee found that “the absence of a statutory basis is an anomaly in Canada’s legislative framework for intelligence.”⁸⁸ Further, the Committee believed that “providing a statutory basis for defence intelligence would entail significant benefits. These benefits include strengthening parliamentary scrutiny over an essentially unknown area of public policy critical to Canada’s security and sovereignty. Clarifying the extent and limitations of DND/CAF authorities; defining key terms; formalizing requirements for inter-departmental consultations; and identifying accountability mechanisms, such as reporting requirements to the Minister, and regular and independent review.” At the same time, the Committee fully recognized that “legislation for defence intelligence activities would have to be carefully crafted to account for DND/CAF’s unique mandate, and its obligations under international law must be taken into consideration.”⁸⁹

In Austria, the activities of both military intelligence services – Military Intelligence Agency (Herresnachrichtenamt) and the Military Counterintelligence Agency (Heeresabwehramt) were not governed by a statute until 2000. The legal basis for their activity was largely derived from a constitutional provision on the army – article 79-1 of the Austrian Federal Constitutional Law.⁹⁰ However, the findings of the parliamentary investigation committee on the Lucona affair triggered a fundamental change in the legal framework and a statute was adopted in 2000 (the so-called Military Powers Act),⁹¹ on which the work of military intelligence agencies is currently based. The investigation committee in particular found that “the competences ... of the military intelligence services related to surveillance have to be determined precisely; due attention has to be paid to respect for relevant provisions on fundamental freedoms and human rights. Bodies of parliamentary control (oversight) of such activities should be provided.”⁹²

In most countries under review, there is no special law governing the activities of military intelligence agencies separately from the rest of the intelligence community. The main provisions on organization, functions and accountability of military intelligence are defined by primary legislation on defence forces or various intelligence/national security service acts. For example, in Estonia, the Estonian Defence Forces Organisation Act regulates the ac-

⁸⁶ In Canada, the activities of the defence intelligence agencies are regulated by the Crown’s prerogative and its administration largely remains within the purview of the executive power. Several normative acts constitute the regulatory framework – the National Defence Act, the Canadian Charter of Rights and Freedoms, the Criminal Code, the Access to Information Act and Privacy Act.

⁸⁷ National Security and Intelligence Committee of Parliamentarians, ‘Annual Report 2018’, p. 98 R7 251.

⁸⁸ Ibid. p.95.

⁸⁹ Ibid. par. 252.

⁹⁰ For an overview, see A. Oschep, 25 Jahre Abwehramt – Entwicklung, Grundlagen und Ausblick’, ÖMZ 1/2011, pp. 48-55.

⁹¹ Bundesgesetz über Aufgaben und Befugnisse im Rahmen der militärischen Landesverteidigung (Militärbefugnisgesetz - MBG), StF: BGBl. I Nr 86/2000.

⁹² Bericht des parlamentarischen Untersuchungsausschusses zur Untersuchung, p. 25 par 4: „die Befugnisse der Staatspolizei und der militärischen Nachrichtendienste zur Überwachung von Personen müssen genau determiniert werden; dabei ist auf die Achtung der einschlägigen Bestimmungen im Bereich der Grundfreiheiten und Menschenrechte Bedacht zu nehmen. Einrichtung zur parlamentarischen Kontrolle solcher Tätigkeiten sollten vorgesehen werden.“

activities of military intelligence agencies in its Chapter 4 – its main tasks, functions, types of intelligence collected, its accountability to the Ministry of Defence, and the coordination of military intelligence by the Security Committee of Government.⁹³ In Hungary, there is a Law on National Security Services which governs the work of all three security service agencies including the Military National Security Service. In Switzerland and Austria as well, the Intelligence Service Act, the Army Act and the Military Powers Act respectively regulate the functions and competences of the military intelligence agencies. A number of countries introduced special legislation on military/defence intelligence, which may also contain provisions on oversight. In Germany, a special law creates the regulatory framework for the activities of the Military Counterintelligence Service (Militärischer Abschirmdienst). Albania has a special Law on Defence Intelligence and Security Agency. Special laws on military intelligence were adopted also in the Czech Republic, Poland, the Slovak Republic, Bulgaria and Denmark among others.

During the last decades there has been growing support in domestic law for governing military intelligence tasks as well as the mandates of oversight institutions in greater detail in primary legislation. Oversight institutions are mostly responsible for oversight of the whole intelligence community including the military intelligence services (Germany, Norway, the Netherlands, Belgium, Montenegro). For example, in Norway, the Act relating to the Monitoring of Intelligence, Surveillance and Security Services regulates the activities of the monitoring body and extends its oversight to defence intelligence.⁹⁴ In Slovenia, the Parliamentary Oversight of Intelligence and Security Services Act regulates all important issues relating to oversight of intelligence agencies covering also the oversight of defence/military intelligence. In Italy, the Law 124/2007,⁹⁵ which was adopted in the course of intelligence sector reform, determines both the organization and powers of the intelligence agencies as well as the mandate and functions of the parliamentary oversight body (Parliamentary Committee for the Security of the Republic⁹⁶ - GOPASIR).⁹⁷ However, the military intelligence agency II Reparto Informazioni e Sicurezza is not integrated into this national security information system.⁹⁸ It is a part of the defence sector, serving narrowly defined defence and military objectives.⁹⁹ Section 8 of the Law 124/2007 clearly defines the mandate of the military intelligence within the system of defence staff: “The Intelligence and Security Department of the General Defence Staff (RIS – Reparto informazioni e sicurezza dello Stato maggiore della difesa) shall carry out exclusively technical military tasks and military police tasks and, in particular, every form of intelligence activity serving to protect the facilities and activities of the armed forces abroad. It shall not be part of the Security Intelligence System. The RIS

⁹³ Riigi Teataja (website), Estonian Defence Forces Organisation Act, Article 10, available at: https://www.riigiteataja.ee/en/compare_original/502072014002.

⁹⁴ The Act relating to the Monitoring of Intelligence, Surveillance and Security Services, available at: <https://app.uio.no/ub/ujur/oversatte-lover/data/lov-19950203-007-eng.pdf>.

⁹⁵ Law no. 124/2007, available at: <https://www.sicurezza nazionale.gov.it/sisr.nsf/english/law-no-124-2007.html>.

⁹⁶ For further details see ‘Il controllo parlamentare’, available at: <https://www.sicurezza nazionale.gov.it/sisr.nsf/cosa-facciamo/i-controlli/il-controllo-parlamentare.html>.

⁹⁷ This has been regarded as a good practice by some commentators: “the best practice that can be identified in the Italian legal regime for the oversight of intelligence agencies is the definition of a clear and precise regulatory framework for the exercise of power by COPASIR,” F. Fabbrini, TF Giupponi, ‘Parliamentary and specialized oversight of security and intelligence agencies in Italy’, in: A. Wills, M. Vermeulen, ‘Parliamentary Oversight of Security and Intelligence’, Annex A, 242 p. 251.

⁹⁸ Ministero Della Difesa, ‘Il Reparto – Informazioni e Sicurezza’; available at: https://www.difesa.it/SMD_/Staff/Reparti/II/Pagine/default.aspx.

⁹⁹ Law no. 124/2007, Section 8 emphasizes the special nature of functions attributed to the intelligence agencies that belong to the Italian Security Intelligence System and determines that these functions “may not be carried out by any other agency, body or office.”

shall act in close association with the AISE,” which is an external security and intelligence agency (L’Agenzia informazioni e sicurezza esterna).¹⁰⁰

3. Objectives of parliamentary oversight

The main purpose of parliamentary oversight is to hold the government to account in different areas of the security sector including intelligence. The historical experience of military intelligence abuse in many countries clearly demonstrates the role of oversight and the culture of accountability within this segment of the security sector. Ideally, parliamentary oversight aims at ensuring a necessary degree of transparency and accountability without putting into question the necessity for secrecy, which is essential for military intelligence effectiveness. Moreover, parliamentary oversight aims at preventing executive abuse of intelligence powers. However, in practice, it is a challenge to exercise preventive (or ex ante) oversight of intelligence services as will be discussed below in more detail. One of the essential functions of parliaments and their standing committees is also to ensure a financial (budgetary) accountability of the executive power and to scrutinise the effectiveness of the intelligence measures and their compliance with the regulatory framework. Arguably, effective parliamentary oversight contributes to more transparency in this sector and strengthens public confidence in the system. Finally, effective parliamentary oversight ensures democratic legitimacy of intelligence services.

4. Tools and mechanisms of parliamentary oversight

4.1 A multifaceted system of oversight

Parliaments have a range of mechanisms at their disposal to exercise oversight over the activities of the military intelligence agencies. Questions related to military intelligence can be addressed in plenary sessions, within the standing defence and security committees and specialized oversight bodies. Furthermore, independent non-political oversight bodies which report their findings to parliament can also significantly contribute to parliamentary oversight of the military intelligence services.

Most standing defence committees under consideration have the power to question the defence ministers on matters related to military intelligence. They can summon the chief of military intelligence and other senior military officials of the armed forces to committee meetings to testify on certain issues. They equally are in a position to hold hearings on military intelligence issues, if necessary. In some cases, the defence committees can serve as a committee of inquiry.

Specialized oversight bodies in parliaments equally play a central role in the process of accountability. They are often in a position to exercise more targeted, operational oversight and may also possess broader oversight competences such as a more comprehensive access to information maintained by the intelligence agencies. Thus, they may be involved in oversight of operations and are complementary to political oversight exercised by the standing defence and security committees of parliaments. The same applies to independent expert oversight bodies, which exercise focused and continued external oversight over military intelligence. Furthermore, there are specialized oversight bodies, which deal with a specific aspect of intelligence activities and their working methods (such as the G-10 Commission in Germany, or independent control mechanisms in Denmark and Belgium). In a number of common law countries, the office of an Inspector-General of Intelligence and

¹⁰⁰ Section 8 par 2 of the Law 124/2007.

Security may play an important role in ensuring accountability of intelligence and security services including military/defence intelligence.

These different tools of oversight are interconnected and build a complex system of oversight. They all play an essential role in the process of accountability.

Various national systems of oversight of military intelligence have been shaped by a range of factors, including the historical experience of military intelligence abuse, constitutional arrangements, the existing practices of accountability in the public sector, and the nature of civil-military relations in the respective country.

4.2 Are the defence committees best placed to exercise oversight?

The tasks of parliamentary defence committees may be relatively complex and multifaceted.¹⁰¹ In some countries, there are committees on defence and security dealing also with broader national security issues and foreign affairs. As military intelligence agencies are increasingly cooperating with a range of domestic and international partners with increasing powers and using a range of sophisticated means of intelligence collection and analysis, it seems at least questionable as to whether the parliamentary defence committees, due to their time and resource constraints, can effectively be in a position to oversee all relevant aspects of military intelligence work - especially the active operations. To a significant extent this depends on the organization, strength, capacities and operations of the respective military / defence intelligence agencies as well as on the existing capabilities of the respective defence committee. In most cases, the oversight exercised by the defence committees needs to be complemented by the oversight of specialized parliamentary bodies and/or non-parliamentary expert bodies, which usually enjoy a greater degree of independence from the executive and the legislature alike. As practice shows, the standing parliamentary committees are primarily responsible for overseeing policy (as well as expenditure and administration) rather than operations.

It has been argued that the risk of politicizing intelligence, time constraints and the lack of expertise in this area are the major drawbacks of general parliamentary oversight. For instance, the EU Parliament advocates to enhance the role of specialized parliamentary committees. The main argument for this is democratic accountability that can to a certain extent be guaranteed through specialized parliamentary oversight. The EU Parliament in its Resolution on renditions “calls the Member States, in the light of increased cooperation and exchange of information between their secret intelligence and secret agencies, to ensure full democratic scrutiny of those agencies and their activities through appropriate internal, executive, judicial and independent parliamentary oversight, preferably through specialized parliamentary committees with extensive remits and powers, including the power to require information, and with sufficient investigative and research resources to be able to examine not only issues such as policy, administration and finances, but also the operational work of the agencies.”¹⁰²

4.3 Organization and composition of oversight bodies

The organization and composition of parliamentary oversight committees may play a crucial role in the exercise of effective and independent oversight. It has been argued that the parliamentary committees in which the majority of members are the representatives of the ruling political party may remain ineffective because they may not be genuinely inter-

¹⁰¹ DCAF Backgrounder, ‘Parliamentary Committees on Defence and Security’, November 2005.

¹⁰² European Parliament, ‘Alleged transportation and illegal detention of prisoners in European countries by the CIA’, 11 September 2012, par 20.

ested in uncovering intelligence wrongdoings. On the other hand, it can equally be argued that this proposition does not fully describe the actual practice, and in a number of cases the oversight committees dominated by the ruling party remain effective in fulfilling their responsibilities. In any case, it is recommended to ensure effective participation of the political opposition in the work of oversight committees. A number of countries under review have done so. For example, Article 105 paragraph 4 of the Croatian Act on the Security and Intelligence System states that “the work of the Parliamentary Committee responsible for national security is chaired by a member of the Parliament, coming from the benches of the largest opposition party.”¹⁰³ Similarly, in Slovakia, the Special Committee on Military Intelligence Service Oversight is chaired by a representative of the opposition party. Some countries institutionalized participation of all political forces represented in parliament (e.g., Slovenia). For instance, in the Netherlands, the Committee for the Intelligence and Security Service includes the minority leaders of all major political parties represented in the House of Representatives.

In Norway, the members of the oversight body – the Norwegian Parliamentary Oversight Committee on Intelligence and Security Services (the EOS Committee), which is responsible for external and independent oversight of all security services including the Norwegian Defence Security Department – are elected by the Storting. Members of Parliament are not permitted to simultaneously serve on the Committee. However, according to the Storting, the composition of the Committee should represent “both political experience and experience from other areas of society”.¹⁰⁴

Such representation can help the oversight committees to keep some distance from government policy in this area and form a more objective view of the situation in the intelligence sector. This is conducive to more independent and objective oversight in general.

In those cases, where there are bicameral systems, the oversight body may include representatives from both chambers of parliament. For example, the Intelligence and Security Committee of the UK Parliament, which is a statutory committee of parliament, not a parliamentary body, and is also responsible for oversight of defence intelligence, may include representatives from both chambers.

4.4 General and specialized oversight bodies

The general and specialized oversight institutions co-exist in many democracies and constitute essential building blocks of the system of oversight. In an ideal case, these different oversight frameworks complement each other. However, they may also overlap in some cases. In general, there seems to be a development towards establishing more targeted oversight frameworks by creating specialized institutions within or outside the parliament. For example, in Slovenia, the Commission for the Supervision of Intelligence and Security Services examines compliance with legal and regulatory requirements. In Poland, the Special Services Committee of the Sejm supervises the Military Counterintelligence Service and the Military Intelligence Service.¹⁰⁵ In line with Article 140 of the Standing Orders of the Sejm, the Committee exercises a range of competences including budget oversight of intelligence services.¹⁰⁶ In Latvia, the National Security Committee of Saeima retains the power

¹⁰³ Security and Intelligence System Act of the Republic of Croatia, promulgated on 30 June 2006, Art 105 par 4.

¹⁰⁴ See the website of the EOS Committee, available at: <https://eos-utvalget.no/en/home/about-the-eos-committee/who-are-we/>.

¹⁰⁵ Articles 137-142 (Chapter 12) of the Standing Orders of the Sejm of the Republic of Poland regulates its composition and the mandate as well as the proceedings in the Committee. The Standing Orders of the Sejm of the Republic of Poland, available at: http://oide.sejm.gov.pl/oide/en/index.php?option=com_content&view=article&id=14798:the-standing-orders-of-the-sejm-of-the-republic-of-poland&catid=7&Itemid=361#23.

¹⁰⁶ “In matters concerning Special Services, the Committee shall participate in proceedings in relation to draft.

to hold to account the Defence Intelligence and Security Service, which is also the national institution of signals intelligence.¹⁰⁷ In Lithuania, the parliamentary Committee on National Security and Defence possesses broad powers to oversee the activities of the military intelligence agency - the Second Investigation Department under the Ministry of National Defence.¹⁰⁸ In Romania, the General Directorate for Defence Intelligence¹⁰⁹ is subject to oversight by the standing parliamentary Committee for Defence, Public Order and National Security, which is generally responsible for overseeing the intelligence activities within the system of the Ministry of Defence.¹¹⁰ In Hungary, the Defence and Law Enforcement Committee as well as the National Security Committee exercise oversight over the activities of the Military National Security Service, which was created as a result of the integration/fusion of the Military Intelligence Office and the Military Security Office on 1 January 2012.¹¹¹

In France, where the parliamentary oversight of intelligence is a relatively recent development (the legal framework was introduced in 2007), the Parliamentary Delegation for Intelligence (Délégation parlementaire au renseignement, DPR) is responsible for oversight of intelligence agencies, while also covering the military intelligence service.¹¹² In Bulgaria, there is a special standing Committee for Oversight of Security Services, the Application and Use of the Special Intelligence Means, and the Data Access under the Electronic Communications Act.¹¹³ The Committee also exercises oversight over military intelligence. At the same time, the standing Foreign Affairs and Defence Committee has the power to hold the Ministry of Defence to account with respect to the activities of the Defence Information Service, also at the Ministry of Defence – Служба ‘Военно Разузнаване’.¹¹⁴ In Croatia, parliamentary oversight “is conducted directly and through the Parliamentary Committee in charge of national security, and the Council for the Civilian Oversight of the Security and Intelligence Agencies.”¹¹⁵

A few countries introduced a more specialized mechanism to supervise military intelligence. In the Czech Republic, it is the Permanent Commission on Oversight that supervises the work of military intelligence. In the Slovak Republic, where military intelligence agencies

budgets and other financial plans of the State as well as consideration of reports on their implementation and shall present its opinion to the appropriate committee.” The material scope of the activities of the Committee are further specified in an appendix to the Standing Orders of the Sejm on the subject matter of activity of Sejm Committees (par 28).

¹⁰⁷ Law on State Security Institutions, Section 14. There is a similar Defence Intelligence and Security Agency with the comparable competencies in Albania, for more details see: <http://www.mod.gov.al/eng/index.php/ministry/subordinate-structures/dia/39-defence-intelligence-agency-dia>.

¹⁰⁸ See the Lithuanian Law on Intelligence (2012). This institution describes itself as the “professional defence intelligence and counterintelligence service which by conducting its activities contributes to national security.”

¹⁰⁹ Romanian Armed Forces military intelligence agency subordinated to the Ministry of National Defence is organized into two directorates: Directorate for Military Intelligence – foreign intelligence; and Directorate for Military Security – counterintelligence.

¹¹⁰ At the same time, there are two joint committees for the oversight of the domestic and foreign intelligence services. The work of the MNSS is governed by the Law on National Security Services (Act CXXV of 1995).

¹¹¹ Tasks of the Military Intelligence Office are defined in Art 6 of the Act 125 of 1995 on the National Security Services. One of the main tasks of the Service is to provide information to the respective state authorities supporting political and military decision-making as well as to ensure the operation of the Ministry of Defence and the Hungarian Defence Forces, and to provide intelligence support and protection to the military personnel serving in international crisis management and peace support operations. For further details see at www.knbsz.gov.hu.

¹¹² For more information, see: <http://www.senat.fr/commission/renseignement/index.html>.

¹¹³ The Committee has nine members, see <https://www.parliament.bg/en/parliamentarycommittees/members/2596>.

¹¹⁴ The Defence Committee has 20 members. For more details see: <https://www.parliament.bg/en/parliamentary-committees/members/2582>.

¹¹⁵ Act on the Security and Intelligence System of the Republic of Croatia, Art. 103-104.

exercise a wide spectrum of activities,¹¹⁶ the main oversight body in the National Council (Parliament) is the Special Committee on Military Intelligence Service Oversight.

Some countries have not yet established specialized parliamentary oversight institutions. In North Macedonia, oversight of the military intelligence service, which forms a structural division of the Ministry of Defence, is a part of the general parliamentary oversight of the defence sector.¹¹⁷ Similarly, in Portugal, the parliamentary Committee on Defence remains a primary oversight body in Parliament responsible for military intelligence. In Sweden, there is no specialized intelligence oversight committee. However, the Committee on Defence and the Committee on Justice exercise oversight of the work of the intelligence service, including defence intelligence (the Intelligence and Security Service). The Committee on Defence reviews government annual reports dealing also with human rights compliance in signals intelligence activities (SIGNINT).

In all these cases, the common tools of political accountability remain applicable, which means that the respective Ministries of Defence can be held to account with respect to military intelligence activities.

Parliamentary specialized oversight bodies may have a broad mandate to exercise oversight. For instance, in Finland, the Intelligence Oversight Committee oversees civilian and military intelligence operations.¹¹⁸ It scrutinizes the effectiveness of military intelligence operations as well as the observance of human rights in such operations. It also deals with the supervisory findings of the Intelligence Oversight Ombudsman.¹¹⁹ Furthermore, the Committee participates in the appointments of the Ombudsman by expressing its opinions to the Government.

A number of countries created not only specialized parliamentary but also non-political external oversight bodies supervising military intelligence. In Denmark, there is a specialized parliamentary committee (the Intelligence Service Committee) that oversees the intelligence services of the Danish police and defence (the Danish Security and Intelligence Service and Danish Defence Intelligence Service). In addition, the Danish Intelligence Oversight Board (TET)¹²⁰ is an independent oversight mechanism which conducts oversight of data collection and processing activities by the Danish Defence Intelligence Service.¹²¹

In the UK, the oversight of defence intelligence is a part of general parliamentary oversight. Defence Intelligence remains accountable to Parliament through the Ministry of Defence (MoD). The Parliament's Defence Committee may scrutinize the activities of the MoD in this area. In addition, there is a specialized statutory (non-parliamentary) oversight body – the Intelligence and Security Committee of Parliament.¹²² It is composed of nine parliamentarians, who are appointed by the Houses of Parliament (having been nominated by the PM in consultation with the Leader of the Opposition).

¹¹⁶ See the competencies of the military intelligence of the Slovak Republic, available at: <http://vs.mosr.sk/o-nas/eng>. See also the Military Intelligence Annual Report 2018, available at: <http://vs.mosr.sk/sprava-o-cinnosti-vs-2018/>.

¹¹⁷ Survey response from North Macedonia, on file with the author.

¹¹⁸ For more information, see: <https://www.eduskunta.fi/EN/valiokunnat/tiedusteluvalvontavaliokunta/Pages/default.aspx>.

¹¹⁹ For more details on the work of the Intelligence Ombudsman, see: <https://tiedusteluvalvonta.fi/en/oversight-of-intelligence>.

¹²⁰ For more information, see: <https://www.tet.dk/?lang=en>.

¹²¹ See, for example, European Digital Rights (EDRI), 'Oversight Board report: Illegal surveillance of Danish citizens', 26 July 2017, available at: <https://edri.org/our-work/oversight-board-report-illegal-surveillance-danish-citizens/>.

¹²² For more information on the Intelligence and Security Committee of Parliament (ISC), see: <http://isc.independent.gov.uk/home>.

In Belgium, there is a Standing Intelligence Agencies Review Committee (Standing Committee I). Its oversight mandate extends to the military intelligence service, the General Intelligence and Security Service. Moreover, there is a special parliamentary Support Commission, with which the Standing Committee I closely cooperates on oversight. Additionally, an administrative commission (Commission BIM) examines the legality of different intelligence working methods and their compatibility with fundamental rights. The Commission is composed of three magistrates.

Thus, there are several models of oversight and various oversight frameworks. In that context, the issue needs to be raised as to how to avoid a fragmentation of oversight or any unnecessary overlap of oversight frameworks. It is essential to introduce a clear separation of tasks and responsibilities and establish a practice of coordination and cooperation between various oversight bodies.

4.5 Case study: The Netherlands – a complex web of oversight

In the Netherlands, a specialized parliamentary committee – the Committee for the Intelligence and Security Services, oversees the activities of the Netherlands Defence Intelligence and Security Service (DISS). Moreover, the Committee is entitled to oversee all aspects of the activities of intelligence services covering lawfulness/legality, effectiveness, efficacy and budget, and has access to all relevant information. The Committee operates in full secrecy.

The Committee on Defence also takes part in the process of accountability. It discusses the public report on the past year's activities, and the annual plan for the running year for the Military Intelligence and Security Service with the Service's Director, followed by a debate with the Minister of Defence.¹²³

Furthermore, there is an expert oversight body – the Review Committee on the Intelligence and Security Services (CTIVD) – which is a specialized oversight body that focuses on scrutinizing the lawfulness of intelligence activities.¹²⁴ The parliament nominates candidates for committee membership and members are appointed by royal decree upon the recommendation by the responsible minister. There are two departments: The Oversight Department and the Complaints Handling Department. The Oversight Department reviews the lawfulness of the activities of the Military Intelligence and Security Service (MIVD) and determines whether the activities of the intelligence service comply with the requirements of the Intelligence and Security Service Act of 2002. The Complaints Department reviews various complaints about the conduct of the MIVD. Furthermore, the CTIVD conducts investigations and monitoring. It has broad investigatory powers and can hear testimony from employees of the service, witnesses, and can also summon expert witnesses. Investigations result in review reports, which contain secret and publicly available sections (the irregularities are mentioned in the publicly available report itself and not only in classified content).¹²⁵

4.6 Relationship between parliaments and specialized oversight bodies

The expert oversight bodies as well as the specialized parliamentary oversight committees can play an important role in providing the parliaments with essential information and assist the legislatures in having an informed debate on military intelligence matters. It remains the responsibility of parliaments to act upon the conclusions of the oversight bodies and to hold the government to account.

¹²³ Survey response from the Netherlands. On file with the author.

¹²⁴ For more information, see: <https://english.ctivd.nl/>.

¹²⁵ N. Verhoeven, 'Parliamentary and specialized oversights of security and intelligence agencies in the Netherlands', in: A. Wills, M. Vermeulen, 'Parliamentary Oversight of Security', p. 257.

The cooperation between parliaments and specialized oversight bodies may have a legal basis or take place rather informally. Arguably, it is a better solution if the cooperation between parliaments and specialized oversight bodies is formalized and institutionalized in legislation.

The parliament may have the power to appoint members of the expert oversight bodies. In Belgium, three members of the Standing Intelligence Agencies Review Committee are appointed by the Senate. In Portugal too, the Parliament elects the Council for the Oversight of the Intelligence System of the Portuguese Republic (CFSIRP)¹²⁶, which is an independent oversight body consisting of three members. It oversees the Intelligence System of the Republic of Portugal (SIRP), monitoring and supervising the military intelligence activities carried out by the armed forces.¹²⁷ The Parliamentary Defence Committee, which oversees defence and military intelligence, can hold hearings not only with the high-ranking officials of the defence and intelligence sector but also with the members of the CFSIRP.

In Germany, the Parliamentary Control Panel (a specialized parliamentary oversight body)¹²⁸ appoints members of the G-10 Commission, a non-parliamentary body, which scrutinizes the use of certain intelligence methods – in particular, the collection and processing of personal data by the intelligence agencies of the Federation, including the Military Counterintelligence Service.¹²⁹ Moreover, the Panel and the Commission have a regular exchange on matters related to their oversight responsibilities.¹³⁰

Another tool used to coordinate and cooperate are respective reporting procedures. The expert oversight bodies may be required to submit regular reports to the parliament or respective parliamentary committees (e.g., Belgium, Canada, UK). Annual reports usually include a section on recommendations and proposed measures that need to be adopted in order to improve the situation (e.g., Slovenia).¹³¹ Moreover, the independent oversight institutions may also cover the follow-up of their recommendations in annual reports (e.g., Belgium).¹³²

However, the interaction between parliaments and specialized oversight bodies (parliamentary or non-parliamentary) may not always be that strong. For instance, with respect to the French oversight body – Parliamentary Delegation for Intelligence (DPR) – one commentator argued that “the DPR has not enhanced Parliament’s information on intelligence issues: the overall knowledge of MPs regarding intelligence activities has not improved: members of the DPR do not communicate with the rest of the Parliament and do not teach other MPs about intelligence”.¹³³

The parliamentary oversight body may be given the power to request the expert oversight body or in some cases, the Inspector General to conduct an inquiry into defence intelligence operations and report back to the parliamentary oversight body (or the parliament). Based on the results of inquiries, the parliaments may take political action, if necessary, for ex-

¹²⁶ For more information on the council, see: <https://cfsirp.pt/en/>.

¹²⁷ Survey response from Portugal, on file with the author.

¹²⁸ Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes, 29 July 2009.

¹²⁹ Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, 26 June 2001, par 15: governs the activities of the G-10 Commission.

¹³⁰ Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, par 15 (8).

¹³¹ In Slovenia, the Commission for the Supervision of Intelligence and Security Services may forward its opinion on a specific issue to the National Assembly and its working bodies, if it deems that these concern important national interests of the state. Moreover, the Commission reports to the National Assembly once a year on its work and on general findings, and proposes the adoption of positions and decisions regarding supervision.

¹³² This is the practice of the Standing Committee I in Belgium.

¹³³ C H. Lepri, ‘Parliamentary and specialized oversight of intelligence and security services in France’, in: A. Wills, M. Vermeulen, ‘Parliamentary Oversight of Security’, 205, p. 211.

ample by putting the respective defence minister under pressure or by raising the issue of political responsibility of the entire government.

Such cooperation can equally take place at the committee level. For example, there is a close working relationship between the Belgian Standing Committee I and the Senate Monitoring Committee, which can ask the Standing Committee I to conduct investigations into intelligence activities. The Standing Committee has to carry out such investigations and report back to the Senate Committee. Some commentators see the expert body oversight in Belgium as a form of democratic control of intelligence services. One commentator argues that “in the existence of this independent, permanent and powerful body (Standing Committee I) lies the strength of the democratic control of the intelligence services in Belgium”.¹³⁴

Croatia represents also a relevant case in this context, where not only parliamentary oversight but also professional oversight exercised by the Office of the National Security Council and civilian oversight exercised by the Council for the Civilian Oversight of the Security Intelligence Agencies were introduced by legislation. In accordance with Art. 104 paragraph 1 of the Law, “the oversight of the Croatian Parliament over security intelligence agencies shall be conducted directly and through the Parliamentary Committee competent for national security, and the Council for the Civilian Oversight of Security and Intelligence Agencies”. The latter is a non-parliamentary oversight body consisting of a chairperson and six members. All Council members and the chair are appointed by Parliament.¹³⁵ They remain accountable to Parliament and the respective parliamentary committee is competent for oversight over the legality of the Council’s work. The Council has to ensure civilian oversight of intelligence agencies and can, among other duties, examine the legality of military intelligence activities. An inspection by the Office of the National Security Council can be initiated at the request of the Parliament or the parliamentary committee responsible for national security.

Thus, it can be argued that defence/military intelligence agencies are subject to various mixed and complementary systems of oversight. All levels of oversight are increasingly interconnected to ensure intelligence accountability. Appointment procedures, regular reporting to parliaments, investigations and inspections carried out by the non-political independent oversight bodies on request of parliaments or parliamentary committees are central elements of accountability relationships between parliament and specialised oversight bodies, enriching parliamentary work on intelligence matters and strengthening parliamentary oversight.

The Council of Europe Commissioner for Human Rights equally recommended in this respect to consider strengthening the link between expert oversight bodies and parliaments by giving a designated parliamentary committee a role in the appointment of members; empowering parliament to task expert bodies to investigate particular matters; and requiring that expert oversight bodies report and take part in hearings with a designated parliamentary committee.¹³⁶ These recommendations to a significant extent reflect the diversity of oversight practice in Europe with respect to military intelligence agencies too.

¹³⁴ W V. Laethem, ‘Parliamentary and specialized oversight of security and intelligence agencies in Belgium’, in: A. Wills, M. Vermeulen, ‘Parliamentary Oversight of Security’, 191, at p. 202.

¹³⁵ For further information on the Council for Civilian Oversight, see: <https://www.sabor.hr/hr/council-civilian-oversight-security-and-intelligence-agencies-6th-term>.

¹³⁶ Commissioner for Human Rights, ‘Democratic and Effective Oversight of National Security Services’, Issue Paper, 2015, par 13.

5. Scope of oversight

5.1 Material scope of oversight

Expertise, capabilities and independence are the preconditions for effective oversight. In addition, the scope of the mandate has to be clearly defined in legislation. Oversight of military intelligence may extend to a range of areas of military intelligence activities and the scope of oversight varies from case to case. The oversight bodies may have the power to scrutinize the legality, effectiveness and appropriateness of certain military intelligence operations. They may be given the power to scrutinize policies as well as spending and administration of intelligence services. For example, the Control Delegation (CD) of the Swiss Parliament, which oversees the activities of the Swiss Federation in the field of military (and civilian) intelligence (in particular the Military Intelligence Service and the Centre for Radio Reconnaissance) focuses on issues related to legality, reasonableness and effectiveness of military intelligence operations. The Control Delegation primarily examines how the executive branch fulfils its supervisory tasks in relation to intelligence agencies. As the Federation Council (the Swiss Government) is responsible for the work of intelligence services, the Control Delegation focuses on the fulfilment by the Council (Government) of its supervisory function in line with the aforementioned parameters for oversight.¹³⁷

In the Netherlands too, the Committee on the Intelligence and Security Services, which is a non-parliamentary oversight body, can address all aspects covering effectiveness, efficacy, lawfulness and budget. However, it has been argued that “in practice, the oversight handles general issues.”¹³⁸ The Standing Committee I in Belgium equally assesses the legality of intelligence working methods and evaluates the effectiveness of intelligence activities as well as the level of coordination between intelligence agencies.

In Norway, one of the main objectives of intelligence oversight is “that the activities are kept within the framework of statute law, administrative or military directives, and non-statutory law.”¹³⁹ The oversight body places a special emphasis on human rights compliance of intelligence agencies, especially with respect to surveillance and personal data gathering.

In line with the Justice and Security Act 2013,¹⁴⁰ the UK Intelligence and Security Committee of Parliament oversees the policies, expenditure, administration and operations of the UK intelligence community including the Defence Intelligence in the Ministry of Defence. The Committee produces annual (and special) reports and conducts inquiries into intelligence operations.

In Australia, the Minister for Defence is accountable to Parliament for the Australian Signals Directorate (ASD), the Australian Geospatial-Intelligence Organisation (AGO), the Defence Intelligence Organisation (DIO). The Australian independent Intelligence Review of June 2017 states that the Minister has “a legal duty as well as a compelling incentive to ensure agencies operate effectively and efficiently, and act with propriety and in accordance with the law.”¹⁴¹ The Australian Intelligence Service Act 2001 determines three functions of the Parliamentary Joint Committee on Intelligence and Security. The Committee reviews the

¹³⁷ Jahresbericht der Geschäftsprüfungskommission und der Geschäftsprüfungsdelegation der eidgenössischen Räte, 28 January 2020, par 4.1 pp. 3034-35.

¹³⁸ N. Verhoeven, ‘Parliamentary and specialized oversights of security and intelligence agencies in the Netherlands’, in: A. Wills, M. Vermeulen, ‘Parliamentary Oversight of Security’, 254, p. 255.

¹³⁹ The Act relating to the Monitoring of Intelligence, Sec. 2 par 3.

¹⁴⁰ Legislation.gov.uk (website), Justice and Security Act 2013, available at: <http://www.legislation.gov.uk/ukpga/2013/18/contents/enacted>.

¹⁴¹ ‘Independent Intelligence Review’, June 2017, p. 112, available at: <https://pmc.gov.au/sites/default/files/publications/2017-Independent-Intelligence-Review.pdf>. Emphasis added.

administration and expenditure of the intelligence agencies, including defence intelligence, and it equally conducts statutory reviews of national security bills introduced to parliament to ensure that national security legislation remains necessary, proportionate and effective.

Some specialized parliamentary oversight bodies monitor the use of special intelligence powers. In Slovenia, the Commission for the Supervision of Intelligence and Security Services of the National Assembly scrutinizes the activities of the intelligence and security service within the Ministry of Defence, and their compliance with the Constitution and the laws as well as with national security policy of the Republic of Slovenia and Government guidelines. It equally supervises the application of legally provided forms, methods and measures for data gathering applied by the defence intelligence service and reports to Parliament once a year on such supervision and provides recommendation on measures to be adopted to improve the overall situation.¹⁴²

In some cases, the domestic legislation explicitly excludes certain areas from the scope of military intelligence oversight. Mostly, this concerns the active operations of (military) intelligence agencies. For instance, in France, the Parliamentary Delegation for Intelligence (DPR) shall not be informed of operational activities of the intelligence services, directives from public institutions and funding, as well as exchanges with foreign and international intelligence services.¹⁴³

5.2 Temporal scope of oversight

In practice, it remains a challenge for various oversight institutions to extend their oversight powers to the entire intelligence cycle, e.g. the collection, analysis and dissemination of information at different stages of the process. This takes place mostly in secrecy and is not subject to preventative or direct operational oversight by the parliamentary standing committees (or the specialized bodies). The standing committees on defence may have a mandate to request the information on certain specific intelligence operations. However, their mandate does not extend to continuous operational oversight of military intelligence measures. Mostly, the parliamentary oversight bodies exercise their mandate in a rather reactive manner, limiting themselves to ex post oversight of intelligence operations. In most cases, the legislatures do not have the power to authorize military intelligence operations.

Parliaments may set up specialized bodies which have the power to authorize the use of certain intelligence methods, for example, in the case of strategic surveillance, which involves the use of signals intelligence – access to communications and metadata (personal data included). It has been argued, however, that “controls have been weaker on account of technical complexity and rapid technological growth of the area.”¹⁴⁴

5.3 Personal scope of oversight

As pointed out above, the parliamentary oversight bodies have the power to hold the respective head of government or the minister of defence to account with respect to military intelligence activities. In some cases, the heads of the military intelligence agencies are also subject to direct oversight by the oversight committees. Thus, in most cases, oversight extends to officials who have the primary political and operational responsibility for military intelligence activities.

¹⁴² For more details, see: <https://www.dz-rs.si/wps/portal/en/Home/ODrzavnemZboru/KdoJeKdo/DelovnoTelo?id-DT=DT009>.

¹⁴³ See also the Spanish Law 11/2002 on the National Intelligence Centre.

¹⁴⁴ Venice Commission, ‘Report on the Democratic Oversight of Signals Intelligence Agencies’, CDL-AD (2015) 011, p. 3 par 4.

In the course of parliamentary inquiries, the activities of a wider circle of military intelligence officials may also be subject to parliamentary and non-parliamentary (specialized) scrutiny.

5.4 Territorial scope of oversight

Military intelligence operations often extend beyond state borders.¹⁴⁵ This enhances the territorial scope of intelligence activities and raises yet another challenge for effective parliamentary (and expert body) oversight.¹⁴⁶ Capabilities of oversight institutions to monitor the protection of basic rights such as the right to privacy in a transboundary context and complex intelligence operations, which usually involve several intelligence actors at domestic and international levels, remain limited.

In some cases, parliaments have the right to be informed of any military intelligence deployments abroad. This is the case in Germany as envisaged by Art 14(7) of the German Law on Military Counterintelligence Service. In line with this provision, the Federal Government informs the Parliamentary Control Panel about the deployment of the Military Counterintelligence Service abroad before such deployment starts. However, no parliamentary approval is required.

6. Parliamentary inquiries

Ideally, an inquiry on defence/military intelligence matters has to be conducted independently and there must be some guarantees that the process will not be overly politicized and its recommendations will be followed. Furthermore, the inquiry commissions should be given subpoena powers and there needs to be clarity as to how the parliamentarians (if they are members of an investigative body) use the information which they obtain during the course of the inquiry/investigation. If the inquiry mechanisms are properly designed and function effectively in practice, they remain a powerful tool at the disposal of national parliaments to hold the executive and its intelligence agencies to account.

The international practice with respect to inquiries on military intelligence matters is very diverse. Such inquiries can be carried out by the standing committees or specialised oversight bodies in parliament. In some countries under review, the defence committees have the power to initiate and carry out inquiries on military intelligence matters (Norway, Germany, Slovenia, Montenegro, Albania, Bulgaria, Croatia, Denmark, Latvia, France, Spain, the UK, Canada). The specialized oversight bodies equally have the power to launch an inquiry. For example, in Italy, a parliamentary oversight body COPASIR (Comitato parlamentare per la sicurezza della Repubblica) is in charge of conducting inquiries on intelligence. The specialized oversight bodies of parliament may be equally entitled to ask another entity to conduct an inquiry. Additionally, an external non-parliamentary oversight body may be given a mandate to carry out such inquiry. In Australia, for example, the Parliamentary Joint Committee on Intelligence and Security, which is constituted under section 28 of the Intelligence Service Act 2001, conducts inquiries into matters referred to it by the Senate, the House of Representatives or a Minister.¹⁴⁷

Ad hoc commissions can be created to conduct an inquiry on a specific matter, or the external (non-parliamentary) oversight bodies can be tasked to carry out an inquiry and report findings to parliament or the respective parliamentary oversight body. In the UK, the De-

¹⁴⁵ MAD-Report: Jahresbericht des Militärischen Abschirmdienstes für das Jahr 2019.

¹⁴⁶ See, for example, a recent Report of the United Nations High Commissioner for Human Rights, A/HRC/39/29, 3 August 2018.

¹⁴⁷ For a complete list of inquiries and reports, see: https://www.aph.gov.au/parliamentary_business/committees/joint/intelligence_and_security/completed_inquiries.

ence Committee, which is a Commons Select Committee and examines the administration, expenditure and policy of the Ministry of Defence and its associated public bodies, has the power to create subcommittees to launch an inquiry into a particular issue of relevance. In Lithuania, the Defence Committee has the competence to launch an inquiry and provide recommendations to the Parliament. In line with the Croatian Parliament's Rules of Procedure, the committee which has jurisdiction over the concrete issue may establish a special ad-hoc sub-committee or working group to exercise further, specifically focused forms of oversight.¹⁴⁸

The plenary may also be entitled to designate or establish a commission to conduct an inquiry. For example, in Norway, the Storting (supreme legislature) can appoint a commission to investigate special cases. In Lithuania, on the proposal of one quarter of members of Parliament, the plenary may designate a committee to carry out parliamentary investigation. In Portugal too, it is the plenary's power to establish a committee of inquiry to conduct parliamentary review or investigation.¹⁴⁹

Furthermore, a parliamentary oversight body may have the power to appoint an expert to conduct an inquiry/investigation, if this is necessary for the fulfilment of its mandate.¹⁵⁰ For example, in Germany, the inquiries can equally be carried out by an authorized representative of the parliamentary oversight body (Parliamentary Control Panel).¹⁵¹

A standing defence committee may have the power to constitute itself as a committee of inquiry. For example, in line with Article 45a paragraph 2 of the German Basic Law, the Defence Committee of the Bundestag shall have the powers of a committee of inquiry. The Basic Law states that "on the motion of one quarter of its members it shall have the duty to make a specific matter the subject of inquiry." In line with paragraph 1 of Article 44 of the Basic Law, the parliamentary committees of inquiry "shall take the requisite evidence at public hearings." However, this requirement does not apply to defence matters. Thus, when the Defence Committee serves as a committee of inquiry, its sessions are closed.¹⁵²

In some cases, there is a broader set of entities dealing with specific aspects of intelligence work. For example, in Canada, the plenary and the Committee both can conduct parliamentary inquiries on military intelligence. Special ad hoc mechanisms have not been introduced for this purpose. At the same time, existing mechanisms that support Parliament, such as the Auditor General of Canada or the Office of the Parliamentary Budget Officer, the Privacy Commissioner or the Information Commissioner could decide on a case-by-case basis to undertake a study related to military intelligence.¹⁵³

The ad hoc commissions of inquiry can be created to deal with a specific intelligence issue. The Venice Commission in its 2007 review of parliamentary oversight mechanisms stated that "parliamentary oversight also carries with it dangers: lack of expertise and professionalism on the part of parliamentarians; leaks to the press or the public of sensitive material. The possibility for the security agency to withhold or conceal information from an 'amateur' investigator means that parliamentary questions or ad hoc parliamentary commissions of

¹⁴⁸ Survey response from Croatia. On file with the author.

¹⁴⁹ Survey response from Portugal. On file with the author.

¹⁵⁰ See Article 7 of the German Law on Parliamentary Control Panel.

¹⁵¹ See, for example: <https://www.bundestag.de/presse/pressemitteilungen/2019/pm-190412-pkgr--635548>. The Parliamentary Control Panel of the German Bundestag can request the Permanent Representative of the Panel to carry out an inquiry.

¹⁵² Several inquiries have been launched and conducted recently. The Kunduz Committee of Inquiry investigated the German air attack in Afghanistan resulting in civilian casualties. The Euro Hawk Committee of Inquiry dealt with the appropriateness of military procurements and trade deals.

¹⁵³ Survey response from Canada. On file with the author.

inquiry usually are only of limited efficacy in this field.”¹⁵⁴ At the same time, the Venice Commission equally stated that “such commissions can be powerful investigative tools in many states, especially if they are provided with considerable powers to obtain necessary classified documentation and to examine witnesses (without restrictions). However, the difficulty in penetrating the intelligence world for parliamentarians not continuously in touch with it can considerably reduce the value of ad hoc parliamentary commissions of inquiry.”¹⁵⁵

The scope of inquiry powers, access to information, subpoena powers and the context in which the inquiry takes place largely determine its effectiveness. The work of the ad hoc committees of inquiry may lead to important changes in the legal and institutional framework. Such structural changes have been implemented in a number of countries as a direct or indirect result of an inquiry.

Not only the parliamentary inquiries but also the inquiries conducted by the external oversight bodies (on their own motion or on request of parliamentary committees or parliaments) may have a significant impact.

An inquiry may raise fundamental questions of democratic legitimacy (or democratic deficit), reveal violations of the law and raise public pressure on the governments and the intelligence community to implement necessary changes within the system. It may also trigger a debate over the role of the respective military intelligence agencies in a democratic society. For example, the 2012 NSU-Inquiry Commission in Germany among a range of other issues scrutinized the role of the Federal Military Counterintelligence Service (MAD), which has been criticized for withholding of important information from the Committee’s scrutiny.¹⁵⁶ This sparked a debate about the role of the agency and the need for reforms.

Furthermore, public inquiries may ensure more transparency and reinforce public confidence in the ability of democratic institutions to oversee the work of intelligence agencies and to enhance the culture of accountability within the intelligence community.

7. Challenges to parliamentary oversight and accountability

7.1 Preventing politicization of military intelligence

It has been argued that “secrecy and clandestine activities may encourage the politicization of the intelligence apparatus, which leads to misuse of intelligence agencies and their special privileges by the executive branch for its own political ends.”¹⁵⁷ At the same time, it is a widely held view that the intelligence shall not be politicized. The services need to demonstrate a considerable degree of political neutrality and independence and be guided by professional considerations. The policy preferences of the government should not influence or determine the intelligence judgments/assessments.¹⁵⁸ This consideration is of special relevance in countries with an abusive military intelligence experience.

¹⁵⁴ Venice Commission, ‘Report on the Democratic Oversight’, par 18. Emphasis added.

¹⁵⁵ Ibid. para 151. Emphasis added.

¹⁵⁶ In particular, the MAD was accused of withholding the information from Parliament about an earlier contact with a right-wing terrorist, a former member of the Bundeswehr who was later involved in terrorist attacks against civilians. In that context some politicians suggested that there is a lack of coordination and accountability in this area. It has equally been argued that the services in their present form cannot be reformed and the MAD should be disbanded altogether. ‘NSU-Untersuchungsausschuss – Verteidigungsministerium: MAD-Akten wurden nicht vorenthalten’, FAZ 12 September 2012. ‘Der Abgrund zwischen den Aktendeckeln’, FAZ 11 September 2012.

¹⁵⁷ FC. Matei, C. Halladay, *The Role and Purpose of Intelligence in a Democracy. Conduct of Intelligence in Democracies: Processes, Practices, Cultures*, Lynne Rienner Publisher, 2019, p. 3.

¹⁵⁸ In any case, a distinction needs to be made between politicization and the guidance provided to the intelli-

However, intelligence does not operate in isolation from politics. Similarly, military intelligence cannot always be kept free from external pressure from defence and military policymakers. This relationship between intelligence producers and the government officials who are supposed to benefit from intelligence products in their decision-making may be a complex one and the degree of politicization varies from country to country. Parliamentary oversight would not always easily penetrate this area. At the same time, as the historical experience shows, political bias of intelligence may significantly undermine public trust in the agencies.

In most cases, parliaments respond in a reactive manner by launching an investigation and creating inquiry commissions to look into a specific issue. As a rule, such commissions provide a set of recommendations to the parliament, which can take certain political decisions and facilitate necessary structural changes. In addition, the legislatures may address the issue of political bias in the framework of their general oversight responsibilities. External specialized oversight bodies that may have more effective access to ongoing operations and be familiar with the internal workings of the services can equally provide their contribution to uncovering such biases within the system.

7.2 Increased cooperation with domestic security services and law enforcement

Military intelligence agencies closely interact with civilian intelligence agencies and law enforcement. Especially in the last two decades and due to the rise of new security threats, a transboundary military intelligence sharing for law enforcement purposes has intensified.¹⁵⁹ A functionally clearly defined relationship between military intelligence and other security or law enforcement agencies in law is essential for establishing clear lines of accountability and ensuring more transparency. Some national legal orders introduce a clear separation between intelligence and law enforcement in legislation. Furthermore, it is equally important to keep a distinction between information sharing for law enforcement and intelligence purposes. This is, however, an area where the division of responsibilities gets increasingly blurred. Moreover, the military intelligence operations such as information collection and analysis need to be clearly separated from decision-making and implementation/enforcement measures in law and practice. In some cases, the dividing lines may not be that clear. It is essential in terms of effective democratic accountability that the mandate of the military intelligence service is clearly formulated in legislation and remains distinct from the tasks of other security services¹⁶⁰ and the law enforcement agencies.

As regards the institutional and functional separation between civilian and military intelligence agencies, it has been argued that “in practice, the line separating the mandates of

gence agencies by the respective intelligence consumers – the respective government agencies and officials. The analytical and other work of intelligence agencies is largely based on such guidance or on the priorities that have in advance been determined by the competent authorities, mostly the governments.

¹⁵⁹ Interpol's Counterterrorism Chief recently stated “the Global Coalition is an example of best practice in sharing military intelligence. I personally believe that the model we developed under the Global Coalition should be copied all over the world, and actually I can tell you we are trying to copy this model, and hopefully by next year we have similar operations ongoing...The methods used during the fight against Daesh are more open and underline the importance of sharing what was formerly seen as ‘secret’ information ... Until recently, the military kept all military intelligence to themselves. But now, in this operation (Operation Inherent Resolve) they de-classify information – not everything of course – just what is necessary to bring awareness and alert the member countries through police channels.” Global Coalition, 5 August 2019, available at: <https://theglobalcoalition.org/en/counter-terrorism-chief-global-coalition-military-intelligence-sharing-method-should-be-copied-all-over-the-world/>.

¹⁶⁰ It may be rather difficult to implement a clear separation of competencies if both military and ‘civilian’ tasks are implemented by the same entity.

military and civilian services is increasingly blurred. Many digital techniques – such as the geolocation of mobile devices – are used by both.”¹⁶¹

7.3 Vaguely defined national security considerations and state secrecy exemptions

In the course of the investigation of practices related to illegal detention of prisoners in European countries by the CIA, the involvement of a number of security and intelligence services in the transportation and detention of prisoners came to public attention.¹⁶² In this context, the issues of democratic accountability of intelligence agencies, secrecy and human rights have been discussed in several international settings. The EU Parliament’s Resolution adopted on 11 September 2012 came to the conclusion that “abuses of state secrecy and national security constitute a serious obstacle to democratic scrutiny.” It stressed at the same time that “in no circumstance does state secrecy take priority over inalienable fundamental rights.”¹⁶³ The parliaments and their defence committees can play an important role in shaping the legal framework for establishing a proper balance between legitimate national security interests and fundamental rights. For example, the independent intelligence review in New Zealand suggested to define the notion of national security in law in greater detail to preclude any misinterpretation in practice. However, the legal provisions cannot cover all conceivable cases, in which the notion of national security can and has to be invoked. For this reason, effective oversight (and judicial authorization procedures) remains essential. The legislation should allow for broader interpretation and application of oversight mandates and limit the space for abusive interpretation and application of the notion of national security.

7.4 Weak internal control mechanisms

The executive and internal control mechanisms play an important role in ensuring effective intelligence accountability in practice. This issue cannot be addressed in greater detail in this review. It suffices to say that internal control mechanisms may be ineffective or biased in some cases. Arguably, the legal recognition of whistle-blowers may to a certain extent strengthen the system of accountability. However, it still lacks recognition in many domestic legal systems across Europe.¹⁶⁴

The practice in the intelligence sector shows that in some cases, whistle-blowers may play a key role in bringing illegal practices or systemic failures to light. For instance, the recent whistleblowing cases in Denmark¹⁶⁵ also demonstrate that sometimes, the system can be brought to account only from within. Therefore, sufficient attention should be paid to devel-

¹⁶¹ EU Agency for Fundamental Rights, ‘Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU’, Vol II, p. 27.

¹⁶² Internationally, special attention has been paid to the Abu Omar case, in which an Egyptian cleric was abducted in Milan and transferred to Germany and then to Egypt. The appeals court in Milan sentenced the former military intelligence chief and his deputy to long-term imprisonment for their role in the case. G. Pianigiani, ‘Italy Jails Ex-Officials for Rendition’, *New York Times*, 12 February 2013, available at: <https://www.nytimes.com/2013/02/13/world/europe/former-italian-military-officials-sentenced-in-abduction-of-abu-omar.html>. See also G. Greenwald, ‘Italy’s ex-intelligence chief given 10-years sentence for role in CIA kidnapping’, *Guardian* 13 February 2013, available at: <https://www.theguardian.com/commentisfree/2013/feb/13/italy-cia-rendition-abu-omar>.

¹⁶³ European Parliament Resolution of 11 September 2012, ‘Alleged transportation and illegal detention of prisoners in European countries by the CIA’.

¹⁶⁴ ‘Protection of Whistleblowers – A Brief Guide for Implementing a National Framework’, Council of Europe 2016.

¹⁶⁵ BBC News, ‘Danish military intelligence head Lars Findsen suspended’, 24 August 2020, available at: <https://www.bbc.com/news/world-europe-53889612>; M Barrett, ‘Why suspension of intelligence chief is a shock in pragmatic Denmark’, *The Local* 24 August 2020, available at: <https://www.thelocal.dk/20200824/why-suspension-of-intelligence-chief-is-a-shock-in-pragmatic-denmark>.

opening a sound legal framework. The primary issue in that context is the extent to which national security whistleblowing must be protected by law.¹⁶⁶ A specific answer to that question can only be provided in national legislation of the respective country.

7.5 Increasing international cooperation and information sharing

Increasing cooperation and information sharing between intelligence agencies poses new challenges to parliamentary and non-parliamentary oversight. It has been argued that parliamentary oversight needs to be designed accordingly and strengthened to meet this challenge and to ensure democratic legitimacy of transboundary intelligence cooperation. For instance, the Reform Commission of the Austrian Army concluded in its 2010 report that it is essential to further develop intelligence cooperation in national as well as international contexts. At the same time, according to this report, it is equally important to develop respective parliamentary control mechanisms.¹⁶⁷

Accountability in this area can be achieved through various channels of oversight. The governments remain primarily responsible for international intelligence cooperation. Parliamentary oversight bodies have the power to hold the respective government to account for certain inter-agency arrangements on intelligence sharing. For example, in Switzerland, the Federation Council (the Swiss Government) has the competence to conclude international treaties on international cooperation in the sphere of military intelligence, in particular, concerning the protection of information or participation in international military information systems. The Federation Council equally regulates the protection of sources and persons, who require such protection due to their intelligence activities. Moreover, the Council determines the framework for cooperation of the military intelligence agency with the foreign services. It approves the inter-agency agreements between intelligence services and ensures that such agreements can only be implemented after approval.¹⁶⁸ The Parliamentary Control Delegation has the power to ensure the accountability of the government for these activities.

Oversight can also be exercised by a non-parliamentary oversight body. For example, in the Netherlands, oversight over the sharing of intelligence across borders is mainly exercised by the expert oversight body – CTIVD. The parliamentary oversight committee limits itself to occasional and general discussions of the issue. It has been argued that as a result of the CTIVD oversight “the assessment framework (with whom may GISS cooperate) and the procedures (what form is the cooperation to take) have gained in quality.”¹⁶⁹ At the same time, the CTIVD proved to be in a position to uncover certain shortcomings in the process of sharing intelligence with international partners.¹⁷⁰

A comparative overview shows that the oversight committees can mostly exercise ex post oversight. The oversight institutions lack necessary competences and capacities to authorize such cooperation or to directly or preventively influence the modalities of cooperation. Limited access to relevant classified information plays a key role in that context – it prevents the overseers from taking a more proactive ex ante stance towards formal or informal

¹⁶⁶ The CoE Guide also points out that “a special scheme or rules, including modified rights and obligations may apply to information relating to national security, defence, intelligence, public order or international relations of the State.” The CoE Guide, p. 27, par 5.

¹⁶⁷ Bericht der Bundesheerreformkommission 2010, p. 50.

¹⁶⁸ Federal Law on the Army and Military Administration of 3 February 1995. Art 99 par 3 bis-6. For further information see at the website of the Independent Oversight Body, available at: <https://www.ab-nd.admin.ch/de/home.html>.

¹⁶⁹ N. Verhoeven, ‘Parliamentary and specialized oversights of security and intelligence agencies in the Netherlands’, in: A. Wills, M. Vermeulen, ‘Parliamentary Oversight of Security’, p. 260.

¹⁷⁰ L. Houwing, ‘Casual attitude in intelligence sharing is troubling’, 12 December 2019, available at: <https://aboutintel.eu/intelligence-sharing-troubling/>.

cooperation arrangements between intelligence agencies. However, at the same time, the relevance of democratic accountability and human rights compliance has been increasingly recognized in various jurisdictions. For example, in Germany, the 2016 intelligence services reform contributed to the strengthening of the regulatory framework, which needs to be reviewed and revised again in light of a 2020 ruling of the Federal Constitutional Court.¹⁷¹ The ruling stressed that a legal framework has to be adopted which imposes a clear legal obligation on the Federal Intelligence Service to obtain the rule of law assurances from the recipient country to guarantee the respect for human rights as well as an adequate level of data protection.¹⁷² The Court equally pointed out that the third-party rule shall not prevent the judicial bodies and the end-to-end overseers from accessing various intelligence cooperation arrangements.

Another recent trend has been to strengthen the information rights of oversight institutions with respect to international intelligence cooperation. It has been argued that parliamentary committees should at least be briefed about new arrangements on intelligence cooperation. For example, in New Zealand, with respect to the Intelligence and Security Act 2017, the “Cabinet has also decided that Parliament’s Intelligence and Security Committee be briefed on any new intelligence relationships for its information.”¹⁷³ On the other hand, it has been equally argued that the advance provision of information to a parliament and/or parliamentary committees may make the legislature complicit in or jointly responsible for government’s potential shortcomings in this area.

A sound regulatory framework is conducive to effective oversight. However, it has been argued that there is a considerable regulatory deficit in this area.¹⁷⁴ The legislatures and their defence committees can contribute a great deal to developing a legal framework, which also incorporates human rights considerations. Domestic law can determine the obligations of military intelligence agencies with respect to international intelligence cooperation and clear cooperation criteria. The mechanisms of cooperation may also be prescribed by the law to a certain degree. In any event, it is essential to enshrine clearly formulated safeguards for data sharing in legislation and implement them effectively in order to protect the right to privacy and freedom of communications.

7.6 Surveillance and personal data processing: the right to privacy

Military intelligence agencies collect, store and transfer information, including personal data. They enjoy broad and intrusive powers that may have a negative impact on fundamental rights. For example, military intelligence agencies may request information from different telecommunication service providers if this is needed for the fulfilment of their mandate.¹⁷⁵

Parliamentary committees may have the power to supervise the use of special intelligence powers. Mostly, the non-parliamentary oversight bodies are set up to deal with a specific aspect of intelligence working methods and their legality or/and reasonableness. These

¹⁷¹ T. Wetzling, ‘Try Harder, Bundestag! Germany has to rewrite its foreign intelligence reform’, 22 May 2020, available at: <https://aboutintel.eu/german-constitutional-court-bnd-ruling/>.

¹⁷² Judgment of 19 May 2020, 1 BvR 2835/17, paras 236-238. See a comment by RA Miller, ‘The German Constitutional Court Nixes Foreign Surveillance’, Lawfare Blog, 27 May 2020, available at: <https://www.lawfare-blog.com/german-constitutional-court-nixes-foreign-surveillance>.

¹⁷³ ‘Arrangements with foreign partners – The sharing of information, technology and expertise with other countries’, available at: <https://dpmc.govt.nz/our-programmes/national-security-and-intelligence-oversight/intelligence-and-security-act-2017/sharing-information/arrangements-with-foreign-partners>.

¹⁷⁴ See, for example, the International Network for Civil Liberties Organizations (INCLO) and Privacy International (PI), ‘Regulate Intelligence Sharing’ 2017, available at: <https://www.inclo.net/pdf/Intelligence-Sharing-Brochure-WEB.pdf>.

¹⁷⁵ See also Art. 8a of the Law on the Domestic Intelligence Service of the Federal Republic of Germany.

oversight bodies are usually requested to present their findings to the respective parliamentary oversight body or the parliament.

Furthermore, it is a primary responsibility of parliaments to introduce a legal framework for surveillance measures and personal data collection by the (military) intelligence agencies. It is crucial to ensure that the legal framework is specific enough as to whether and under what circumstances intrusive intelligence measures have to apply. The legal framework should enshrine certain procedural safeguards and introduce a system of advance judicial authorizations of such measures (judicial authorizations are not the subject of this review). Moreover, the mechanisms need to be created to effectively oversee intelligence activities and to prevent any abuse of intelligence powers.¹⁷⁶

Internationally, a special emphasis has been placed on the role of “mixed models of administrative, judicial and parliamentary oversight.”¹⁷⁷ It has been argued that “parliamentary committees also can play an important role; however, they may also lack the independence, resources or willingness to discover abuse, and may be subject to regulatory capture.” It has further been pointed out that the “jurisprudence at the regional level has emphasized the utility of an entirely independent oversight body, particularly to monitor the execution of approved surveillance measures.”¹⁷⁸

It has been argued that there is a growing accountability deficit in times of increasing trans-boundary intelligence cooperation and there is a need for enhancing and internationalizing the oversight mandates.¹⁷⁹ There have been some initiatives to draft the common principles governing the working methods of intelligence agencies. However, they have not yet produced concrete results.

7.7 Preventing complicity in mistreatment by foreign services

Intelligence sharing may lead to illegal action against individuals resulting in grave violations of human rights such as torture, detention without trial, or extrajudicial killing. A fundamental challenge for intelligence agencies including military intelligence remains how to mitigate the risks of such violations by foreign services. In some cases, the services are required to obtain assurances against mistreatment and to attach certain conditions to the information to be passed.¹⁸⁰ However, it has been called into question as to what extent the process of assurances can be seen as a reliable and adequate means of mitigating concerns about torture and ill-treatment.¹⁸¹

As for now, a few countries have developed standards and policies on intelligence sharing with foreign services. Applicable norms and procedures may be defined by legislation or in

¹⁷⁶ See, for example, the Special Report on the Collection, Use, Retention and Dissemination of Information on Canadians in the context of the Department of National Defence and Canadian Armed Forces Defence Intelligence Activities, issued on 12 March 2020 by the NSICOP (The National Security and Intelligence Committee of Parliamentarians), available at: https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-sr/special_report_20200312_public_en.pdf.

¹⁷⁷ ‘The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights’, A/HRC/27/37, 30 June 2014, par 37. See also a recent report: ‘The Right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights’, A/HRC/39/29, 3 August 2018.

¹⁷⁸ A/HRC/27/37, 30 June 2014, par 38. Emphasis added.

¹⁷⁹ T. Falchetta, ‘Enhance and internationalise the oversight mandate’, About Intel, 8 October 2019, available at: <https://aboutintel.eu/enhance-the-oversight-mandate/>.

¹⁸⁰ Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees (July 2010), par 24. See also: HM Government. The Principles relating to the detention and interviewing of detainees overseas and the passing and receipt of intelligence relating to detainees, (July 2019), par 20.

¹⁸¹ R. Blakely, S. Raphael, ‘Recommendations for reform of the Consolidated Guidance’, 25 October 2018.

policy documents. For example, in the UK, consolidated guidance and principles relating to the passing and receipt of intelligence relating to detainees have been developed. In Canada, the Avoiding Complicity in Mistreatment by Foreign Entities Act (2019) was adopted, which is “an act respecting disclosure and request for information that would result in a substantial risk of mistreatment of an individual by a foreign entity and the use of information that is likely to have been obtained as the result of mistreatment of an individual by a foreign entity.” In addition, there are ministerial directions dealing with this issue and addressing the Department of National Defence as well as the Canadian Armed Forces.¹⁸²

In particular, the Ministerial Direction to the Department of National Defence and the Canadian Armed Forces prohibits “a. the disclosure of information that would result in a substantial risk of mistreatment of an individual by a foreign entity; b. the making of requests for information that would result in a substantial risk of mistreatment of an individual by a foreign entity; and c. certain uses of information that was likely obtained through the mistreatment of an individual by a foreign entity.” If that risk of mistreatment cannot be mitigated in a specific case, in line with the Direction, information will not be shared with the respective foreign service.

Generally, in most countries, the situation seems to be somewhat more complex and problematic in the field of military intelligence, where the information is often shared in the context and in support of multilateral military operations. Additional challenges for oversight may arise in this context. A broader range of issue need to be considered when developing a regulatory framework. One of them is the extent of applicability of the rules and procedures on due diligence and risk assessments to military intelligence agencies. A sound risk assessment framework should be put in place. Decision-making procedures should be defined, and authorization responsibilities allocated at different levels. Furthermore, it should also be clarified what mechanisms for following up on the assurances received from foreign entities apply and how and to what extent those assurances can be enforced. Compliance with the standards should be reviewed regularly and the role of parliamentary oversight and other review bodies clarified.

It has repeatedly and correctly been pointed out that “transparency as to the circumstances in which intelligence agencies will share information and the procedures governing such sharing” should be guaranteed.¹⁸³ It remains a task for national legislatures to enact legal standards in this area through legislation.

In any case, it is recommended to develop a regulatory framework and further guidance at the national level, which will also be applicable to military intelligence agencies, and to provide adequate (mandatory) training for military intelligence officers who are responsible for sharing information with foreign entities. On the other hand, it would equally be useful to

¹⁸² Ministerial Direction to the Department of National Defence and the Canadian Armed Forces, ‘Avoiding Complicity in Mistreatment by Foreign Entities’, 24 November 2017, available at: <https://www.canada.ca/en/department-national-defence/corporate/ministerial-directions/avoiding-complicity.html>. It “requires that a classified annual report be provided to the Minister regarding its application, and that an unclassified version be released to the public.” See also: Deputy Minister of National Defence and Chief of the Defence Staff, ‘Directions for Avoiding Complicity in Mistreatment by Foreign Entities’, 19 September 2019, available at: <https://www.canada.ca/en/department-national-defence/corporate/ministerial-directions/directions-for-avoiding-complicity-in-mistreatment-by-foreign-entities.html>. The 2017-18 Annual Report on the Ministerial Direction to DND/CAF emphasizes the role of the Defence Intelligence Oversight Board (DIOB), which is “the most senior DND/CAF integrated board providing guidance, policy direction and decisions related to the management of defence intelligence including information sharing arrangements,” available at: <https://www.canada.ca/en/department-national-defence/corporate/ministerial-directions/2017-18-annual-report-avoiding-complicity-mistreatment-foreign-entities.html>.

¹⁸³ Privacy International, ‘Policy Briefing – UK Intelligence Sharing Arrangements’, April 2018.

improve military expertise and knowledge in the respective oversight bodies that are directly responsible for ensuring effective oversight and accountability for intelligence sharing.

This topic cannot be fully addressed in this paper; however, it can be maintained that there remain considerable regulatory and implementation challenges. Only time will tell whether military intelligence cooperation and information sharing will be accompanied by more regulation in the future aimed at achieving a greater degree of transparency and accountability in this area of public policy.

8. Parliamentary participation in decisions on appointments

The powers of parliamentary committees regarding nominations and appointments of military intelligence officials remain rather limited. In the majority of cases under review, the standing defence committees do not directly participate in high-ranking military intelligence appointments; neither do they approve the maximum number of personnel employed by the military intelligence nor the human resources management plan for the military intelligence.¹⁸⁴

The parliamentary committees do not directly take part in high-ranking military intelligence appointments in Canada, Belgium, Denmark, France, Italy, the UK, Germany, the Netherlands, Portugal and Spain. However, in some cases, they are consulted by the Minister of Defence regarding such appointments (Lithuania, Latvia, Bulgaria, Croatia, Montenegro, the Czech Republic, Poland). Such consultations may have different meanings in different cases.

As a rule, the committees are consulted prior to appointments. However, there are also cases where the defence or other standing committees hold a hearing after appointment. For example, in Bulgaria, the Defence Committee was consulted twice in the last two years.¹⁸⁵ In particular, the Minister of Defence presented the newly appointed head of the Defence Information Service to the Committee. The head of the Defence Information Service is appointed for a term of five years by decree of the President on the proposal of the Council of Ministers. The legislature can hold a hearing of the appointed head of the Service after his/her appointment. Thus, the Committee's power to influence the appointment process itself remains rather limited.

In a few cases, the Defence Committees (Lithuania) or the Special Services Committees (Poland) are entitled to submit opinion on proposed candidates and approve high-ranking military intelligence appointments (Latvia, Lithuania, Montenegro, Croatia). In Hungary, the Defence Committee holds a hearing to form an opinion on the suitability of the suggested candidates for the post of Director General of the Military National Intelligence Service.¹⁸⁶ In Montenegro, the chief of the military intelligence section in the Ministry of Defence is appointed by the Government on proposal of the Defence Minister and after obtaining an opinion from the competent working body of the Parliament, e.g. the Security and Defence Committee.¹⁸⁷

The appointments can be subject to politicization in some cases. In particular, the question as to who should lead the respective military intelligence agency – a civilian or a member of

¹⁸⁴ Based on survey findings on file with the author.

¹⁸⁵ Survey findings from Bulgaria.

¹⁸⁶ See also the survey findings from Lithuania and Hungary, on file with the author.

¹⁸⁷ Art. 41 of the Law on Defence; see also the survey findings from Montenegro. The Committee has 11 members and exercises a wide variety of tasks related to defence and security sectors. For further information, see: <http://www.skupstina.me/index.php/en/odbor-za-bezbjednost-i-odbranu/about-the-working-body>.

the military forces – may be contested.¹⁸⁸ One may argue that it is necessary for a civilian head of the military intelligence agency to possess some military qualifications. At the same time, it has also been argued that a civilian head of military intelligence would be amenable to political influence from different sides and such influence would largely be considered incompatible with the mission and functions of military intelligence. On the other hand, it can equally be argued that, depending on the defence architecture in the respective country, it is not absolutely necessary to appoint a military person to the post, and a well-qualified civilian may also be in charge. It depends on the status and responsibilities of the respective entity: whether it is a part of the armed forces; its main tasks; and the type of personnel it employs.

9. The power of the purse / budgetary issues and expenditure

One of the areas of oversight where the parliaments and their defence committees play a central role is the legislature's power of budget oversight. The parliamentary defence committees may be in a position to influence the budgeting process at an early stage of drafting. However, they may not have access to all budget documentation/information related to military intelligence agencies. In some cases, specialized parliamentary oversight bodies have the power to monitor financial operations of the military/defence intelligence agencies. For example, in Slovenia, the Commission for the Supervision of Intelligence and Security Services may request the Government to submit a report on financial operations of the intelligence services.

In a number of countries, there is a designated parliamentary body responsible for financial affairs of security services and intelligence agencies. In Germany, there is a Confidential Committee of the Budget Committee of the Bundestag, which approves the operating budgets of the federal intelligence agencies including the Military Counterintelligence Service. Its members are elected by the Bundestag for the duration of the legislative period. Another function of the Confidential Committee is to scrutinize as to how the funds allocated to the three federal intelligence services (including the Military Counterintelligence Service) are being spent. The Confidential Committee has comprehensive oversight functions (comparable to those of the Parliamentary Control Panel). The Confidential Committee and the Parliamentary Control Panel closely cooperate and coordinate the process in order to avoid any accountability gaps and to ensure effective oversight. In line with section 10a par 2 of the Federal Budget Code: "For compelling reasons of secrecy, the Bundestag may in exceptional instances make the authorization of expenditures that are to be managed under operating budgets ... The Federal Ministry of Finance shall submit the operating budgets for the intelligence services to the Confidential Committee for approval".¹⁸⁹ In the Spanish Parliament (Cortes Generales), there is la Comisión de Control de los Créditos Destinados a Gastos Reservados (the Committee for Control of the Credits for Reserved Expenses), in short - La Comisión de Secretos Oficiales (the Committee of Official Secrets).

One of the major advantages of similar specialized budget oversight mechanisms is their comprehensive access to all relevant information at different stages of the budget process and their ability to continuously oversee spending. Another important feature is their accountability to parliament. For example, the German Confidential Committee submits reports to the Bundestag twice during a legislative period.

An independent scrutiny of military intelligence finances and spending can also be exercised by the independent audit bodies. Under certain circumstances, such mechanisms

¹⁸⁸ 'Bulgaria changes law to allow civilian to head Military Intelligence', The Sofia Globe 26 July 2019, available at: <https://sofiaglobe.com/2019/07/26/bulgaria-changes-law-to-allow-civilian-to-head-military-intelligence/>.

¹⁸⁹ More on the Confidential Committee (Vertrauensgremium), see: https://www.bundestag.de/ausschuesse/weitere_gremien/vertrauensgremium.

can be seen as an important aspect of parliamentary oversight. For example, the Swedish National Audit Office under the Riksdag (parliament) carries out independent audits of intelligence-related state finances and reports to the Riksdag.¹⁹⁰ The Auditor General, who leads the work of the Office, is appointed by the Swedish parliament. The Office carries out financial as well as performance audit. As a part of such performance audit, the Office scrutinizes the efficiency of state institutions and as the Office website states, “it can relate to that the operations of the authority are not cost effective, that they have inefficient organisation or that they are not observing rules and ordinances.”¹⁹¹ In 2015, the Office implemented an audit of the Swedish Defence Intelligence operations¹⁹² and published a report, in which the purpose of the audit was clearly formulated – to “assess whether SIUN’s (the Swedish Foreign Intelligence Inspectorate) control of defence intelligence operations is effective.”¹⁹³ It is equally interesting to have a look at the questions on which the audit was based. The Office raised the following questions: “Has the Government created conditions for effective control activities? Are the control activities conducted effectively? Does the control agency report the results of its control as intended to the defence intelligence agencies and to the Government? Do decisions resulting from controls lead to action by the defence intelligence agencies?”¹⁹⁴ This element related to follow-up actions by the defence intelligence agencies is of key importance in other countries too. It seems to be less formalized and institutionalized in a number of cases under review and can be regarded as a missing link in a complex system of defence/military intelligence accountability.

Due to the secrecy of intelligence budgets and non-disclosure of their contents, it is of key importance to ensure a minimum degree of transparency and democratic accountability for spending. This can to a significant extent be achieved by a combination of the intra-executive branch oversight with (specialized) parliamentary oversight. The power to allocate military intelligence budget funds remains with parliament in many cases. However, it is questionable as to what extent parliament and sometimes also their defence committees or specialized bodies can directly and proactively (preventatively) influence military intelligence spending. What the parliamentary oversight bodies can still do is to monitor and oversee (control) such spending from time to time and make recommendations or raise questions of legal or political responsibility of the respective decision-makers. Contrary to this, the specialized (parliamentary) oversight bodies can access relevant military intelligence budget documents and information (including classified materials) and exert influence at an early stage of budget drafting.

The level of detail at which oversight bodies can oversee the military intelligence budget (programs, projects, line-items) depends on the nature of the oversight and the specialization of the respective oversight body, and varies from country to country. However, in most cases under consideration the standing defence committees do not have the power to supervise military intelligence budgets at this level of detail.¹⁹⁵

¹⁹⁰ In other countries too, budgetary oversight is exercised by the audit services. For example, in the Netherlands, the Court of Audit and the National Audit Service are responsible for such oversight.

¹⁹¹ See Swedish NAO webpage, available at: <https://www.riksrevisionen.se/en/about-the-swedish-nao/fields-of-operation.html>.

¹⁹² Defence intelligence operations are run by the Armed Forces, the National Defence Radio Establishment, the Swedish Defence Research Agency and the Defence Material Administration.

¹⁹³ Swedish National Audit Office, ‘Audit Report – Summary, Control of defence intelligence operations’ (RiR 2015:01), p. 1.

¹⁹⁴ Swedish National Audit Office, ‘Audit Report’.

¹⁹⁵ Survey findings on file with the author.

10. Parliamentary participation in decision-making on procurements

Most parliaments and parliamentary defence committees do not directly oversee procurements made by military intelligence agencies. However, in some cases, depending on the overall number of procurements, parliamentary approval and/or participation in decision-making may be required. For example, in Lithuania, the Minister of Defence or the Chief of Military Intelligence is obliged to provide the Defence Committee with detailed information on procurement decisions above 20 million euro. Moreover, the Committee has a right to request information during all stages of the procurement process and to submit its opinion.¹⁹⁶ In Bulgaria, such information has to be provided to the Committee and the parliament when a decision on procurement above 50 million euro is made.¹⁹⁷ The parliaments and defence committees have similar powers in the Netherlands, Denmark, Portugal, Montenegro and Latvia. In Canada and Latvia, the standing committees are involved in specifying the need for new equipment as well.

Parliamentary oversight over financial operations carried out by the defence sector including military and defence intelligence agencies can be exercised through an independent body such as the audit offices in some instances, which are accountable to the parliament and accordingly, regularly provide the parliamentarians with their findings and recommendations. Parliaments can subsequently take a follow-up action and hold the executive to account, if necessary.

11. Access to information

11.1 Access to information and its limitations

The parliamentary (or external) oversight bodies need to have effective access to classified information to be able to exercise oversight.¹⁹⁸ In some cases, the oversight bodies possess broad rights to access or obtain information from the military intelligence agency. However, depending on the scope of their competencies and functions, they may have full or partial access to classified information on military intelligence. This also depends on the level of classification of information in the respective country.

The parliamentary oversight (defence) committees have the power to obtain documents from the military intelligence services in a number of countries (the Czech Republic, Slovenia, Poland, Norway, Turkey, Montenegro, Albania, Canada, Belgium, Bulgaria, Croatia, Denmark, France, Latvia, Lithuania, the Netherlands, Portugal, Spain, Germany). In some cases, they equally have a right to request and receive the information, including the classified information, or an assessment on a specific topic or military intelligence operations. Additionally, an oversight institution (a defence committee or a specialized oversight body) may request the military intelligence agency to keep parliament or the defence committee regularly informed on their activities (Slovenia, Bulgaria, Hungary). However, the scope of

¹⁹⁶ Survey response from Lithuania.

¹⁹⁷ Survey response from Bulgaria.

¹⁹⁸ See some examples of good practice in the Report of the Special Rapporteur on the protection and promotion of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/14/46, 17 May 2010, practice 7: "Oversight institutions have the power, resources and expertise to initiate and conduct their own investigations, as well as full and unhindered access to the information, officials and installations necessary to fulfill their mandates. Oversight institutions receive the full cooperation of intelligence services and law enforcement authorities in hearing witnesses, as well as obtaining documentation and other evidence."

information which is accessible to parliamentary (or non-parliamentary) oversight bodies differs from case to case.

A leak of classified information to members of parliament, the broader public or the media has been considered as a risk and an obstacle to trust-building and effective working relationships between the oversight committees and the military intelligence community. However, this should not serve as an argument against giving full access to relevant information to the committees responsible for oversight. The national legal frameworks introduce certain mechanisms that minimize the risk of a leak such as vetting (security-screening). However, in some cases, the national legislation adopts the doctrine of parliamentary privilege, which means that the members of the standing parliamentary committee responsible for oversight cannot be subject to any security-screening. State practice varies in this respect.¹⁹⁹ In some cases, the members of oversight institutions sign certain non-disclosure agreements. Furthermore, the national legislation may impose an obligation on members of an oversight body not to disclose information they receive when fulfilling their oversight duties (Belgium).

There remain important areas of military intelligence work where the relevant information remains undisclosed or access to information is limited.²⁰⁰ These areas include military intelligence cooperation with partners, information on specific (active) operations, information concerning sources, intelligence work methods, and its capabilities. Certain aspects of military intelligence work such as the working methods or the means used can be subject to some kind of scrutiny or authorization by an independent body (or judicial authorization).

11.2 Access to information on ongoing operations

Some national legal orders introduce explicit limitations to access to information on the intelligence working methods and sources of intelligence information. In Spain, the Law 11/2002 regulating the National Intelligence Centre states in Article 11 that the respective oversight committee of the Congress of Deputies “shall have access to knowledge on classified matters, except those related to the sources and resources of the National Intelligence Centre and those stemming from foreign services and international organizations according to the terms laid down in the relevant agreements and conventions on the exchange of classified information.” There are similar provisions in other legal systems. For instance, in Latvia, “the National Security Committee of the Saeima (Parliament of Latvia) is entitled to hear reports and statements of the heads of state security institutions, as well as to get acquainted with the official documents and information of such institutions, except the documents on confidential sources of information.”²⁰¹

As regards the information related to ongoing operations, there are a few explicit limitations in national legislation. In France, the law regulating the work of the parliamentary oversight body explicitly excludes ongoing operations as well as international intelligence cooperation from the scope of its mandate.

¹⁹⁹ Good practice suggests the following:

“Oversight institutions take all necessary measures to protect classified information and personal data to which they have access during the course of their work. Penalties are provided for the breach of these requirements by members of oversight institutions.” Report of the Special Rapporteur on the protection and promotion of human rights and fundamental freedoms while countering terrorism. Martin Scheinin A/HRC/14/46 (2011), practice 8.

²⁰⁰ In line with the Tshwane Principles, “governments may legitimately withhold information in narrowly defined areas, such as defence plans, weapons development, and the information and sources used by intelligence service. Also, they may withhold confidential information supplied by foreign governments that is linked to national security matters.” Principle 9, Global Principles on National Security and the Right to Information (The Tshwane Principles), 12 June 2013.

²⁰¹ Law on State Security Institutions, Sec 25 par 3.

It is not only a purely legal question as to whether certain information can or should be published. Sometimes, the political context and the specific circumstance of the case may also play a decisive role. When there is a matter of great public interest on the agenda of the oversight committee or public inquiry, the executive authorities may come under increased pressure to disclose relevant information. However, the respective government may or may not provide such information to the respective oversight body. For example, in the Russia investigation in the UK, the Intelligence and Security Committee raised this issue in the final report on Russia presented to the public. In this report, the Committee stated the following: “We remind the Government that the Justice and Security Act 2013²⁰² does not oblige it to withhold information relevant to ongoing operations but merely provides the option of doing so. The Agencies and the departments are able to provide any information relating to an ongoing intelligence or security operation voluntarily. Whilst we would not expect to receive highly sensitive current operational material in most cases, it is disappointing that in relation to a subject of such public interest, this option has been exercised quite so broadly.”²⁰³ Thus, in some cases, the executive retains some flexibility to disclose or not to disclose information relevant to ongoing operations.

11.3 Access to information on intelligence cooperation and sharing

In line with the Council of Europe Human Rights Commissioner’s recommendations, access to information by oversight bodies should not be “restricted by or subject to the third-party rule or the principle of originator control. This is essential for ensuring that democratic oversight is not subject to an effective veto by foreign bodies that have shared information with security services. Access to information by oversight bodies should extend to all relevant information held by security services including information provided by foreign bodies.”²⁰⁴

However, in practice, overseeing transboundary intelligence sharing constitutes a serious challenge for parliaments and standing parliamentary committees. Military intelligence sharing regularly takes place. However, specific national regulations or publicly accessible military intelligence sharing agreements are rather an exception in state practice (agency-to-agency agreements often remain out of the public eye).²⁰⁵ Parliamentary ratification of respective agreements is not yet an integral part of states’ treaty practice. If they exist, their implementation remains a challenge.²⁰⁶ In some cases, the legislation explicitly excludes international cooperation between intelligence agencies from the scope of parliamentary oversight (France, Spain). At the same time, there is a trend of increasing parliamentary involvement in overseeing international intelligence sharing and cooperation. Moreover, efforts have been made to organize cooperation between different national oversight institutions across borders in order to overcome the existing democratic accountability deficit in this area.²⁰⁷

²⁰² Main functions of the Intelligence and Security Committee are defined in Justice and Security Act (2013), available at: <https://www.legislation.gov.uk/ukpga/2013/18/section/2/enacted>.

²⁰³ Intelligence and Security Committee of Parliament (presented to Parliament pursuant to section 3 of the Justice and Security Act 2013), ‘Russia’, 21 July 2020, par 90 at pp. 27-28.

²⁰⁴ CoE Commissioner for Human Rights, ‘Democratic and Effective Oversight of National Security Services – Issue Paper’, 2015, par 16. Emphasis added.

²⁰⁵ ‘South Korea and Japan to extend military intelligence-sharing agreement’ 22 December 2019, available at: <https://www.thedefensepost.com/2019/11/22/south-korea-japan-military-intelligence-sharing-extend/>. See also ‘Turkey, Kazakhstan agree on military cooperation that covers intelligence sharing, defence industry’, Nordic Monitor 16 May 2020, available at: <https://www.nordicmonitor.com/2020/05/turkey-kazakhstan-agree-on-military-cooperation-that-covers-military-intelligence-defence-industry-and-joint-projects/>.

²⁰⁶ See, for example, on the practice in the Netherlands: L. Houwing ‘Casual attitude in intelligence sharing is troubling’, 12 November 2019, available at: <https://aboutintel.eu/intelligence-sharing-troubling/>.

²⁰⁷ One of such attempts is the establishment of the so-called Club de Bern. See L. Jirat, ‘Club de Bern: a black box of growing intelligence cooperation’, 1 April 2020, available at: <https://aboutintel.eu/the-club-de-berne/>.

11.4 Access to information on intelligence measures with adverse human rights impacts

It has been recommended to disclose to the respective oversight bodies information “relating to areas of activity that are deemed to present particular risks to human rights, as well as any information relating to the potential violation of human rights in the work of security services.”²⁰⁸ The Tshwane Principles also state that “there is an overriding public interest in disclosure of information regarding gross violations of human rights and serious violations of international humanitarian law.”²⁰⁹ Furthermore, “information regarding other violations of human rights or international humanitarian law is subject to a high presumption of disclosure, and in any event may not be withheld on national security grounds in a manner that would prevent accountability for the violations or deprive a victim of access to an effective remedy.”²¹⁰

Military intelligence agencies may get involved in a range of activities that have immediate human rights implications not only for military members, but also for civilians. The agencies collect the data, including the personal data and under certain circumstances may also get involved in different forms of surveillance. Surveillance activities as well as collecting and handling (personal) data may involve serious risks of violations of human rights. It is a challenge for parliamentary oversight bodies to exercise effective oversight. Arguably, the independent (non-political) specialized oversight bodies may be better placed to exercise oversight in this area than parliamentary oversight institutions. Several countries under review introduced specialized monitoring mechanisms that in some cases are accountable to the parliaments or the standing parliamentary committees.

12. Follow up of recommendations arising from oversight

In many cases the findings of the oversight bodies are of recommendatory nature and do not produce legal obligations on the part of the executive to act. However, this cannot be extended to all oversight, control or authorization mechanisms. For example, certain inquiry commissions may be in a position to issue legally binding decisions. Moreover, specialized bodies that authorize the use of special intelligence methods can also issue binding decisions. Furthermore, although the findings of a parliamentary or external oversight body may not be legally binding for the government, they may be authoritative enough to induce the executive to take action in response to findings that arise from parliamentary or independent oversight. Such findings may even lead to certain legal and institutional reforms in the respective country.

Non-compliance with recommendations may have political, legal or reputational consequences for government and intelligence services. In most of the countries under review, the general tools of government accountability can be activated if necessary.²¹¹ For example, in the Netherlands, the House of Representatives can adopt a motion of distrust, which will force the defence minister to resign. Similarly, in Poland, motions requiring a vote of no confidence can be initiated. In the UK, the House of Commons could vote down or amend the defence budget. In Lithuania, the defence committee can summon the Defence Minister to initiate interpellation in a parliamentary inquiry. The plenary may express no confidence in the Prime Minister or the Minister. In Latvia, the competent parliamentary committee can

²⁰⁸ CoE Commissioner for Human Rights, ‘Democratic and Effective Oversight of National Security Services – Issue Paper’ 2015, par 17.

²⁰⁹ Global Principles on National Security and the Right to Information (The Tshwane Principles), 12 June 2013, 10 A (1).

²¹⁰ Ibid. 10 A (2).

²¹¹ Survey findings on file with the author.

address any non-compliance; it may ask Prime-Minister or the Minister of Defence to resort to administrative or disciplinary measures depending on the obligations violated or mismanagement uncovered by the oversight institution. In Denmark, if a majority in the parliament loses faith in the Minister, they must resign. Under conditions of minority government, this may be an effective means of exerting pressure. Thus, parliaments can take action on the basis of oversight findings. Furthermore, the structural problems revealed by a parliamentary or independent (non-parliamentary) inquiry within the system of military intelligence may lead to certain legislative and institutional changes. The role of parliaments and their standing committees remains of key importance in that context.

13. Change of modalities of operations

The oversight bodies do not have the power to directly influence ongoing intelligence operations. However, parliaments and their standing committees can use general oversight powers to influence modalities of ongoing military intelligence operations (if they are aware of such operations). For instance, in Canada, the Parliament has the power to draw attention to matters of military intelligence by debating motions, asking questions of the government in Question Period or in Committee, submitting written questions, calling for documents, or initiating a committee study on a specific topic.²¹²

Oversight institutions need access to relevant information and facilities to be able to make a specific assessment of the situation and demand a change. For example, in Latvia, the parliamentary committee can request information relevant to ongoing military intelligence activities and may call for a change in operations.²¹³ However, parliamentary requests for a change of modalities of intelligence operations may also be based on relevant information provided by a specialized non-parliamentary oversight body (or media reports).

14. Ending the military intelligence operations

Most parliamentary and non-parliamentary oversight bodies do not have a power to end military intelligence operations as such. They may demand to end certain military intelligence measures, but such demands would not be binding on the executive. However, oversight institutions can influence the decisions to end military intelligence operations through various channels. In most cases, parliament's role would be to investigate and if necessary, propose changes to the broader structures of military intelligence, as opposed to specific measures.

We have a different picture if we take a look at the role of specialized bodies in authorizing and scrutinizing the use of certain intelligence techniques. For instance, in Belgium, there is a Commission BIM, which supervises the application of certain intelligence working methods and examines their compatibility with fundamental rights. In France too, there is an independent administrative authority – the National Commission for the Control of Intelligence Techniques – which issues opinions on the authorization given by the Prime Minister to the intelligence agencies to use certain intelligence techniques. Additionally, the National Commission equally carries out a posteriori control of the collection and storage of the data resulting from these techniques. Thus, similar bodies could in principle significantly influence the practice of the use of certain intelligence techniques and review their lawfulness.

²¹² Survey response from Canada, on file with the author.

²¹³ Survey response from Latvia, on file with the author.

Conclusion

The parliamentary oversight bodies need to be seen in the context of the multifaceted systems of oversight frameworks that have been introduced in a number of countries under review. Their functions and competences cannot adequately be assessed without taking into account the specificities of the system as a whole and its structure.

The present paper gives just an overview over the different systems of oversight and attempts to identify some commonalities and trends as well as some accountability deficits within the system. In certain areas, parliamentary oversight remains relatively weak – these include active intelligence operations as well as transboundary intelligence sharing and cooperation.

National parliaments conduct much of their oversight of military intelligence services through their standing defence and national security committees. At the same time, specialized parliamentary bodies and non-political external oversight institutions have been increasingly responsible for overseeing the operations of military intelligence agencies.

Attempts have been made to enhance and institutionalize cooperation between different oversight frameworks – parliamentary oversight committees and non-parliamentary oversight bodies. In most cases, defence committee oversight focuses on policy and budgetary issue while specialized parliamentary or non-parliamentary independent oversight bodies oversee operations, dealing with questions related to the lawfulness and effectiveness of such operations.

Cooperation and coordination between parliamentary and non-parliamentary oversight bodies should further be institutionalized and strengthened. At the same time, a fragmentation of oversight or any unnecessary overlap of different oversight frameworks, which may create additional obstacles to intelligence accountability, should be avoided.

Conclusion. Parliamentary Oversight of Military Intelligence: Recommendations

Dr Teodora Fuior, DCAF — Geneva Centre for Security Sector Governance

Introduction

For oversight to be credible it needs to be based on clearly defined legal authority, embedded in the Constitution and laws, and meeting the democratic standards that make checks and balances functional, and accountability a fundamental principle of governance. However, legal authority is not sufficient for effective oversight. The parliament must have the ability to utilize the legal powers it has and transform them into oversight action, and it needs to do this routinely. For this to happen, oversight committees need staff, information, expertise, and well-defined rules of engagement in oversight.

Here are some strategies that aim to better enable committees to make full use of their legal authority and engage in effective oversight of military intelligence.

1. Clarify the regulatory base of military intelligence

Most often, military intelligence is one (or a few) sub-organization(s) within the defence ministry and the armed forces, thus they do not have their own statutory law; their mandate is briefly and generally provided for in a few articles of the law on defence.²¹⁴ The organization of military intelligence, their mandate and powers are, in most countries, regulated not by laws adopted by parliament, but in subsidiary regulations approved by the executive. These by-laws are often not public.

Further on, military intelligence employs both civilian and military personnel, and are under a double subordination - to the civilian political leader (the minister of defence) and to the military leader (chief of staff). Their mission encompasses a range of activities from data collection and analysis to deploying uncover agents and combat units, carrying out strategic reconnaissance, running security background checks for MoD personnel, and ensuring the protection of classified information and of intelligence personnel across the defence establishment. They have the legal authority to intercept communications and sometimes even to conduct cyber counterattacks.²¹⁵ These activities are conducted in compliance with a range of international regulations and national laws, such as defence law, the status of the military personnel, national security law, protection of state secrets, interception of communications, international humanitarian law (law of armed conflicts), rules of engagement, and local laws in the theatre of operations.

Effective oversight of military intelligence must start with a very clear inventory of military intelligence functions, missions and powers. Those must be correlated with existing national

²¹⁴ One notable exception is the German Military Counterintelligence Service (Militärischer Abschirmdienst, MAD), which is a part of the German armed forces but have their own statutory law dated from December 1990.

²¹⁵ For example, see the case of Belgium military intelligence service GISS, Wauter van Laethem: Intelligence oversight in the 21st century, 'The Rule of Law and 25 years of intelligence oversight in an ever-changing world: the Belgian Case', Routledge, 2019, pg. 110. See also 'Enquête de contrôle', 2007.181, Committee I, p.5, available at: https://www.comiteri.be/images/pdf/eigen_publicaties/rapport_181_%20fr.pdf.

legislation, and eventual gaps must be addressed in a legislative development plan. 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 jeopardize the work of military intelligence services and/or national security if made public (such as operational methods and the use of particular devices or technologies).

2. Improve committee access to information

Most European parliaments have privileged access to classified information to enable them to oversee intelligence agencies. Parliament's right to be informed by the executive represents the first condition for effective law making and oversight.

In security and intelligence matters, the access to information raises challenges linked to the need to balance the imperatives of democratic accountability and transparency with the requirements of security and state secrecy. Confidentiality limits the flow of information towards the parliament and the public. However, distinction must be made between the "need for confidentiality," which is understandable and manageable, and its extreme interpretation which is the "lack of public scrutiny," which is unacceptable in democracy.

Generally, intelligence and security oversight committee have access to classified information. The circumstances and conditions of this access must be clearly defined by law and rules of procedure. There are two main ways to grant MPs this access: (1) without a security clearance (as an exception to the statutory rules on access to state secret information); or (2) after receiving a security clearance.

In a majority of European countries, it is assumed that the elected nature of the parliamentary mandate entitles MPs to have access to classified information, without any background verification.²¹⁶ It is considered that a vetting process of MPs would be a violation of the separation of powers; it would restrict membership in oversight committees and potentially lead to obedience to the executive. A secrecy oath taken after being elected to a committee that deals with defence, security or intelligence is necessary and sufficient for getting access to state secrets, if this is justified by the committee mandate. This access to classified information does not mean that MPs are exempt from legal sanctions for unauthorized disclosure of secret information.

In other parliaments, committee members obtain access to classified information only after receiving a security clearance (some examples are Estonia, Hungary, Latvia, Lithuania, Serbia and North Macedonia). The security clearance is issued by Parliament or by the National Security Authority after MPs undergo background checks performed by a governmental agency (most often the domestic intelligence service). The vetting provides a risk assessment referring to underlying affiliations, interests or vulnerabilities which could lead individuals to disclose classified information for money, political or business interests or through blackmail. A successful formal vetting process is a confidence-building mechanism. Building trust in the relationship between oversight bodies and intelligence agencies is especially needed in young democracies, where security agencies are very reluctant to share information. The vetting process clarifies the rules of the game and empowers MPs in their dialogue with executive officials.

The access to information related to military intelligence might however raise problems in both models presented above. Security clearances are in some countries required for exceptional circumstances, even when MPs access to classified information is normally

²¹⁶ For example, see the case of the Netherlands, available at: <http://www.ennir.be/netherlands/intelligence-review-netherlands>.

granted. Such exceptional circumstances often relate to parliamentarians' access to foreign classified information (Norway, Estonia, Croatia, Romania) or to 'top-secret information' (Poland).

There are several risks to be mitigated when MPs are vetted:

- There is a potential conflict of interest if the 'overseen' is also the 'gate keeper' for access to information by overseers. Most often the background security checks for MPs are conducted by the domestic intelligence service - which is supposed to be subsequently overseen. In such cases, intelligence agencies may excessively and arbitrarily delay the vetting process or deny the security clearance for some parliamentarians, interfering with the committees' composition. To mitigate this risk, the agency which does the checks should only issue an opinion, but they should not be the ones who decide on issuing the security clearance. The final decision should be taken by Parliament and the law must provide for appeal mechanisms in cases where a clearance is denied.
- Creating two classes of parliamentarians in the oversight committees: those with, and those without clearance (because they failed the vetting, or because they refused to apply). This can jeopardize the functioning of the committee and the credibility of parliament as overseer. To mitigate this risk, the vetting can be done before the committee is formally established, to clear all prospective members; only MPs who get the clearance should be appointed to the committee.
- A security clearance does not completely prevent an unauthorized disclosure of classified information. Politicians do not necessarily have a secrecy culture or a clear understanding of legal consequences and operational implications of unauthorized disclosure. However, consistent dialogue between parliament and the services builds up awareness and responsibility. In most states, parliamentarians do not enjoy immunity from prosecution in the case of an unauthorized disclosure of information.

Box 8. How is committee access to information regulated in some countries?

- Germany - the Parliamentary Control Panel has the right to request information, documents and other data files from the Federal Government and the three intelligence services. Demands must be met immediately. Staff of the intelligence agencies can also be questioned. Control Panel's members are sworn to secrecy; they can comment publicly on certain issues if the decision to do so is reached by two-thirds of its members. Control Panel may request expert witnesses to submit evaluations. (Parliamentary Control Panel Act)
- Romania – The Intelligence Oversight Committee (for the domestic service SRI) can request reports, briefs, explanation, documents, data and information; they can summon military and civilian personnel of the service to hearings. SRI is obliged to submit the information requested to the Committee within seven working days; if the deadline is overdue SRI is obliged to explain the reasons and say how much time will be needed to prepare the requested information. (Parliament Decision No. 85/2017)
- Hungary – two-thirds of National Security Committee can vote to require the executive or an agency to disclose specific information concerning the intelligence agency's methods. (Act CXXV/1995)

With or without a security clearance, parliamentarians need to know that total access to classified information is unachievable. There are two interlinked limits to access: the mandate of the committee and the need-to-know principle.

A committee's access to information must be defined by its oversight mandate. The needs for information of a committee that deals with issues of policy and legality are different to those of a committee mandated to oversee the efficiency of intelligence operations – which requires more in-depth information. This relationship is important not only for providing committees with the information needed to fulfil their mandate, but also for preventing MPs' attempts to access information that may be unrelated to their work.

The need-to-know principle addresses the same issue: even if someone has all necessary official approvals, they should not get access to specific information unless they have a need to know that information - with need justified by the conduct of the person's official duties. This principle aims to discourage free "browsing" of sensitive material or the misuse of classified information for personal interests.

These limits on access to sensitive information demonstrate again that committee mandates must be very well defined in law and rules of procedure. If the parliament does not do this, the responsibility (or discretion) to define the need to know of a parliamentary committee falls completely on the executive. As a consequence, the parliament's access to information depends on ministerial discretion, and the parliament may have limited or no procedure for challenging such decisions.

Most often, laws define the exceptions from access and not the categories of information that can be shared by the service with the oversight committee. This ensures more access to information for parliament, as all information that is not exempt has to be made available to the committee. The most frequent exceptions from access are the following:

- Information pertaining to ongoing operations. Any disclosure of operationally sensitive information might compromise the operation and endanger the officers who implement it. However, MPs should be aware that some operations might be ongoing for years, remaining impermeable to oversight; or it might be difficult to determine when an operation has finished. The assessment belongs to the agency and this margin of discretion can be manipulated to hide information from the gaze of the committee. Besides this, sometimes there is a grey area between policy and operations (e.g. patterns of targeting and targeting priorities).
- Information relating to sources and methods used. Identities and roles of human sources are among the most sensitive aspects of intelligence work. Leaks of source identities can jeopardize their personal safety whereas dissemination of information about methods could render methods ineffective, give advantage to adversaries and endanger individual human sources. Sometimes however, when the committee has a mandate to investigate suspected serious criminality (such as corruption or human rights violations) access to this kind of information might be necessary.
- Information from foreign entities. This is the result of international intelligence cooperation (information sharing and joint operations). Restrictions are based on the "third party rule"²¹⁷: before passing the information to a third party the agency must request permission from the originating entity. There is little data available on how often such requests are made and if they are successful. The sharing of information between intelligence agencies has increased exponentially over the past decade, international cooperation having become one of the main sources of intelligence information.

²¹⁷ Sometimes referred to as 'originator control' (ORCON).

Without information about international intelligence cooperation, committees have an incomplete view of activities involving their own State's agency. Getting more information about international cooperation (or even being exempt from the third-party rule) is an endeavour of many oversight bodies in Europe.

- Information on judicial proceedings or criminal investigations - restrictions are applied in order to safeguard both the right to a fair trial and the State's ability to investigate and prosecute crime. They ensure oversight bodies do not examine matters that are subject to criminal or judicial investigations until the investigations have been completed.

Box 9. 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 establishes 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 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.

The 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 and develop sufficient fact-finding ability to effectively investigate conduct and records in the possession of intelligence agencies.

Box 10. How can the 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 - these are 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 of 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.

3. 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 a deep knowledge of security and intelligence issues are comparatively rare. In almost every circumstance the intelligence services have the upper hand in terms of expertise, access to information and freedom of decision making over their process, tasks and resources. Oversight is heavily dependent on the executive and the services' willingness to share information and "educate" MPs about intelligence activity.

Developing expertise, knowing what to look for and what questions to ask is a precondition for effective oversight. Committee members and staff advisors need to develop a good understanding of the law, policy and functions of intelligence services, and to be able to apply this knowledge in considering whether the services are meeting the requirements of democracy, human rights, and due legal process. One can distinguish several types of expertise required in intelligence oversight.

- Democratic oversight expertise – a good understanding of the importance of oversight and the function of parliament in a democracy; knowledge of oversight tools; familiarity with parliamentary and committee procedures. The work of parliament, the legislative procedures, the function of committees, and their role within the system of checks and balances that make democratic accountability possible is unique, and difficult to grasp for outsiders. Before learning about the particularities of the intelligence world, committee members (especially new MPs) need to understand and internalize the principles and the modalities of democratic oversight, develop the attitude, the political will and the courage necessary for engaging in meaningful oversight activities.
- Legal expertise – a clear understanding of the strategic framework and all relevant law and regulations underpinning intelligence activity in the country. This should include laws and procedures governing:
 - The remit and mandate of all intelligence services.

- Human rights, privacy and civil liberties, and when these can be infringed upon for national security reasons.
 - The use of special powers such as the recruitment of agents or interception of communications.
 - Data protection.
 - Citizen complaints, and complaints of service employees, including what protections exist for intelligence staff, such as protection from illegal orders or whistle-blower protection.
- Operational expertise – an understanding of how services really function. Whether committee members have prior experience of military and intelligence matters or not, they should all strive to understand the intelligence function in a modern state. This should include:
 - The different realms of state intelligence, considering civil, military and law enforcement dimensions; and questions of domestic and overseas intelligence gathering.
 - The main forms by which information is collected and then analysed, such as: human intelligence (HUMINT); interception and communications intelligence (COMINT); open-source intelligence (OSINT); imagery intelligence (IMINT); covert surveillance operations; and cyber operations, both defensive and offensive.
 - Acknowledging the principles and mechanisms for cooperation with partners overseas.
 - Understanding which agencies and bodies are responsible for these various activities; what is the relationship between them; how responsibilities and priorities for intelligence-gathering are determined within the intelligence sector.
 - Technological expertise - the understanding of technological matters and their rapid evolution especially information and communications technology (ICT) and data management. Parliamentarians cannot make correct legal assessments if these are based on wrong assumptions of how technology works. We live in an increasingly digitalized society that produces vast, previously unimaginable amounts of data. Technology and advances in artificial intelligence provides security services with a plethora of new opportunities.

Box 11. Expertise available to oversight bodies in UK

Intelligence and Security Committee of Parliament (ISC) - composed of 9 MPs, selected from a list approved by the Prime Minister, with appointments agreed with the Leader of the Opposition, including candidates from both houses of the assembly. The committee members must ideally have some prior experience of intelligence matters, but cannot be a serving government minister, as is the case in many parliamentary systems. For administrative support in running inquiries and producing reports, the UK's ISC members draw on permanent staff within the National Security Secretariat in the Cabinet Office.

Investigatory Powers Commissioner's Office (IPCO) constitutes an amalgamation of separate commissioners' offices into one with the passing of the Investigatory Powers Act (IPA) in 2016. IPCO has the responsibility for overseeing the daily intelligence activities of all bodies and agencies exercising investigatory (i.e intelligence gathering) powers. This includes a set of judges (called Judicial

Commissioners) who provide the “double-lock” sign-off on interception warrants, as newly mandated by the IPA of 2016. In all, the IPCO comprises:

- 15 Judicial Commissioners
- Approximately 50 administrative and technical staff presenting a range of expertise including legal and technological.
- An ad hoc Technology Advisory Board (TAB) which can be pulled together as required to comment on particular areas of technical complexity. This body includes a range of government personnel, academics, and technical experts from industry, including those working in information and communications technology (ICT). The group does not sit permanently but can be called-together at least once per year, and more often as specific requirements demand.

In this way, the IPCO provides both day-to-day oversight of intelligence activities and a deeper set of expertise to supplement the work of the parliamentarians in the ISC.

Acquiring expertise in this field is a slow process, requiring dedication and persistence. MPs should have realistic expectations and ambitions in the process. It is generally accepted that it takes probably 18-24 months to understand the functions and technicalities of intelligence, and this is dependent on the services’ willingness to cooperate and share information. Given the inevitable turnover of committee members after elections, the development of a strong expert staff capacity within the parliament is essential. In the absence of staff, committee’s research possibilities are limited, obliging members to rely mainly on information provided by the government and the security agencies, the very institutions the committee must oversee.

Committee staff prepare and organize committee meetings, maintain contacts with government agencies, collect information and help interpret government information. They must cover a wide range of activities, from secretarial work to juridical advice, drafting legislation, planning and organizing oversight activities, drafting reports, research papers, or speeches. Stable professional staff is essential to enable committees to meet their responsibilities; they ensure the continuity of expertise and the institutional memory of a committee.

Box 12. Sources of enhanced committee oversight ability

- Access to information
- Clear and detailed committee procedures
- Parliamentary staff: use of four circles of inner expertise:
 - Personal advisors
 - Parliamentary group staff
 - Committee staff
- Specialized departments (e.g. the Parliamentary Centre, legislative department)
- The use of external expertise: academia, NGOs
- Cooperation with other oversight bodies: National Audit Office, Ombudsman, Data Protection Agency

4. Clarify committee procedures

Parliamentary procedures (often called ‘Standing Orders’ or ‘Rules of Procedure’) are a set of rules, ethics, and customs governing meetings and other activities of Parliament. The Rules of Procedure (RoP) are adopted by Parliament in its plenary session, at the beginning of each legislative term. Their aim is to facilitate the smooth and efficient functioning of parliament and provide a basis for resolving any questions of procedure that may arise, taking into account the rights of its members. The general principles of parliamentary procedure include the rule of the majority with respect for the rights of the minority.

The mandate and the working practices of most parliamentary committees is briefly defined in laws and in the general RoP of the Parliament. This gives them sufficient legal authority to carry out their mandate. However, committees with an especially sensitive and difficult mandate, such as intelligence oversight committees, may have their mandate and oversight powers defined in detail by a special Parliamentary Decision – which gives them more legitimacy and confidence while engaging in oversight, since it shows the support of the whole Parliament for their mandate.

Committee Rules of Procedure are adopted by committee members at the beginning of the committee’s mandate, to better define their mandate and enable a smooth functioning of the decision-making process within the committee. They usually refer to:

- The mandate should describe the issues and/or institutions in the committee’s area of competency. The committee RoP would need to be updated (and voted upon) frequently, at any change of institutional design or name in the committee’s area of competency. As the committee develops its expertise and understanding of intelligence networks and activities, they might want to broaden or redefine their mandate and the methods of engaging with overseen institutions.
- The rights and responsibilities of the chairperson, deputies and staff.
- The procedure for calling and running a committee meeting including the size of quorum (important for avoiding blockages from the chairperson if they are the only one left in charge).
- The rules of debate and vote must ensure that minority groups can express their views and participate in decision making processes.
- The possibility of having a member represented by other colleagues in case of unavoidable absence.

Box 13. How do parliamentary oversight committees organize their work?

- Adopt committee RoP.
- Clarify their mandate and priorities: legislation or oversight; policy, budgets or operations?
- Decide on the profile of the administrative and expert staff they need; convince Parliament to allocate sufficient funds to the committee to employ the required experts (for both permanent and temporary support)
- Establish subcommittees and/or appointing rapporteurs dedicated to the oversight of one particular institution or issue (such as the implementation of committee recommendations, a specific law or reform). They have the responsibility to monitor respective issues and regularly inform the committee on its progress; plan and organize concrete oversight activities; ensure regular communication on the issue; and identify committee needs for external expertise.

- Identify independent sources of information and expertise outside the intelligence sphere and executive: academia, national and international think tanks, civil society organisations, etc.
- Considering what oversight tools to use in order to gain a good understanding of intelligence structures and processes: request briefings and follow-up reports from the agencies; organize field visits and inspections, call intelligence personnel to hearings; address questions and interpellations in the plenary; plan for the utilization of specific oversight tools according to specific oversight objectives and priorities.
- Decide on an Annual Activity Plan to facilitate planning; engagement of expertise, and communication with intelligence services.
- Establish good connexions with the media: identify journalists with interest and knowledge on security matters who are willing to report about committee activities with professionalism and objectivity.

5. Organize joint meetings and oversight activities

Most parliaments put in place several parliamentary and eventually non-parliamentary bodies with competency for military intelligence legislation and oversight. The composition, tasks, workload, transparency and objectives of these bodies varies. There are often overlaps between their mandates, but there might also be aspects of intelligence work that slip in-between, enabling the services to avoid meaningful oversight if they choose. Therefore, communication, expert collaboration and joint action between committees are indispensable for several reasons.

- Understanding intelligence better. The intelligence sector is complex, and intelligence services do not act in isolation. The responsible committees must make a realistic assessment of the state of the intelligence sector and how it reacts to the security environment in its totality. The traditional division of labour between intelligence agencies is challenged by today's trans-border security threats. There is an increased integration of executive responses to threats, intense cross-government and international intelligence cooperation, blurred lines between intelligence functions, or between the public and private use of information as a consequence of the use of contractors. Oversight has developed institutionally, with parliamentary committees focused on specific government departments, but what is required today is functional oversight. In other words, parliament needs to develop a comprehensive understanding of processes and networks involving all those who develop security-related intelligence.
- Pooling resources and expertise. The resources (staff, time, budgets) for oversight are always very small compared with the resources of those being overseen, therefore, it is vital that resources are leveraged in order to have more impact. The expertise developed by each committee and their experience in engaging in effective oversight needs to be shared with others. This is a small step towards rectifying the information asymmetry among the intelligence services and the parliament.
- Creating increased political leverage. Working together, committees can better influence the executive and the intelligence sector. Committees have no power of enforcement; their recommendations are not legally binding on the executive; they have to rely on the force of argument, on publicity and on multi-partisan support to convince the parliament to follow their advice and the executive to comply with their recommen-

dations. When acting together, committees have increased legitimacy and their united voice has considerable political weight.

For these reasons, developing cooperation and complementarity of action between defence and security, law enforcement and intelligence committees is essential for effective oversight.

It is the right and responsibility of the committees to define when (the situations) and how (the procedures) they should work together and join forces in oversight. This can be decided upon:

- Informally and ad-hoc, after discussions between committee chairpersons and members, in order to jointly debate and analyse an overarching policy, strategy or piece of legislation (such as national security strategy, law on communications interception, the status of military personnel, the status of intelligence officers, etc.) or investigate a matter of common interest and organize joint hearings of public officials, or joint study visits and inspections in the field.
- Formally, cooperation can be provided for in the Rules of Procedure of each committee. The RoP of each committee should describe the situations and the procedures for joint meetings, after consultations among the committees in order to create similar and convergent provisions. In time, after joint committee meetings become an established practice, Rules of Procedure for joint committee meetings can be developed.
- The committees dealing with security and intelligence oversight should also develop the practice of sitting with other committees, on case-by-case bases, to discuss policy, legislation or joint oversight action.

The key principle in organizing oversight activities should be that a holistic and results-based approach should be taken (Venice Commission, 2015). The important question is not what sort of, or how many oversight bodies are established, but whether the result is effective oversight.

DCAF Geneva Centre
for Security Sector
Governance



NATO PARLIAMENTARY ASSEMBLY
ASSEMBLEE PARLEMENTAIRE DE L'OTAN

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

✉ info@dcaf.ch

☎ +41 (0) 22 730 9400

www.dcaf.ch

🐦 [@DCAF_Geneva](https://twitter.com/DCAF_Geneva)