DCAF Geneva Centre for Security Sector Governance

Assembly of the Republic of North Macedonia

GUIDELINES FOR INTELLIGENCE OVERSIGHT

for parliamentary committees in the Assembly of the Republic of North Macedonia

January 2021

FORWORD AND ACKNOWLEDGEMENTS

The *Guidelines for Intelligence Oversight* was first published in May 2018 at the request and for the use of the three parliamentary committees mandated to oversee the security and intelligence sector in the Parliament of the Republic of North Macedonia. Since 2018, rapid and important changes have been made within the Macedonian intelligence accountability system. New institutions were created, and new regulations were enforced, requiring an adaptation of oversight processes. During 2020, we have undertaken an overhaul review of the *Guidelines* text, drafting a revised edition which reflects all these reforms.

From the very beginning, the development of the *Guidelines* was a remarkable collective effort that involved both the authors of the text and the prospective readers.

As co-authors of the first edition of the *Guidelines,* **Magdalena Lembovska, Dr. Julian Richards** and **Wouter de Ridder** brought into the text the valuable and diverse perspectives of a researcher, a former senior intelligence manager and an oversight practitioner. The text was enriched and aligned to the new legal and institutional context with the remarkable individual and collective effort of **Igor Kuzevski, Dr. Ice Ilijevski**, and our colleagues from DCAF office in Skopje: **Vlado Gjerdovski** and **Dr. Kire Babanoski**.

Elected members and parliamentary staff advisors from the three parliamentary committees responsible for intelligence and security oversight have provided us feedback every step of the Guideline development, from the definition of its content to the comprehensive review of the text that produced this second edition. We are especially grateful to the members of the **Assembly of the Republic of North Macedonia** who took time out of their busy schedules to discuss with the authors and to share with us perspectives from which we learned a great deal.

The **Belgian Federal Parliament** kindly supported this publication through the active involvement of the Standing Intelligence Agencies Review Committee (Committee I) in a sustained exchange of good practice and lessons learned with colleagues from the Republic of North Macedonia.

The *Guidelines* reviews the Macedonian legislative framework and oversight system, and it provides information on international principles and good practices in intelligence oversight. Designed to inform and support parliamentary committees in fulfilling their oversight mandate, since its first publication the *Guidelines* was used by DCAF as reference in over 20 workshops and practical exercises organized for the Macedonian parliamentary committees. At their turn, the committees directly utilized the *Guidelines* in conceptualizing and planning oversight activities which contributed to an uncontested improvement of parliamentary performance in intelligence and security oversight. We hope that this revised version of the *Guidelines* will respond to the expectations and needs of the new members of the Assembly, continuing to serve as a useful and informative tool for their work.

Dr. Teodora Fuior, lead author
Geneva, January 2021

Funded by UK Government
Kingdom of the Netherlands
Sweden Sverige
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Federal Department of Foreign Affairs FDFA
Swiss Agency for Development and Cooperation SDC

ABOUT DCAF

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice and supports capacity- building of both state and non- state security sector stakeholders.

DCAF's Foundation Council is comprised of representatives of about 60 member states and the Canton of Geneva. Active in over 80 countries, DCAF is internationally recognized as one of the world's leading centres of excellence for security sector governance (SSG) and security sector reform (SSR). DCAF is guided by the principles of neutrality, impartiality, local ownership, inclusive participation, and gender equality. For more information visit www.dcaf.ch and follow us on Twitter @DCAF_ Geneva.

DCAF - Geneva Centre for Security Sector Governance
Maison de la Paix
Chemin Eugène-Rigot 2E
CH-1202 Geneva, Switzerland
Tel: +41 22 730 94 00
info@dcaf.ch
www.dcaf.ch
Twitter @DCAF_Geneva

CONTENTS

1

INTRODUCTION

1.1 THE RELEVANCE OF INTELLIGENCE OVERSIGHT IN A DEMOCRACY

Parliamentary oversight refers to the ongoing[1] 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.

Parliamentary oversight must extend to all areas of government, including intelligence and security services. Intelligence services work in secrecy and have the authority to make use of special powers that potentially are highly invasive of human rights. Communications interception and secret surveillance are only two of such powers. For these reasons, intelligence services are regarded by the public with suspicion and lack of confidence. Therefore, the need for legality, legitimacy and accountability is even higher for intelligence services than for other government agencies.

› WHAT ARE SOME OF THE SPECIAL POWERS OF SECURITY AND INTELLIGENCE SERVICES?

- To tap, receive, record and monitor conversations, telecommunication, other data transfer or movement – within the country or from abroad.
- Conduct secret surveillance, record, and trace information.
- Searching enclosed spaces and intrusion into property.
- Opening letters and other consignments, without consent of the sender or addresser.
- To request providers of public telecommunication networks to furnish information relating to identity of users and the traffic taking place.
- Exploiting software for clandestine entering, copying or corrupting databases ('hacking').
- Having access to all places for installation of surveillance.
- Collecting financial information on individuals or networks.
- Recruiting and managing secret human resources.
- Using false legal entities for the support of operational activities.

As the lawmaker, parliament is responsible for enacting clear, accessible and comprehensive legislation establishing intelligence services, their organisation, special powers and limits. Parliamentary oversight activities review, evaluate and investigate how laws are implemented and how intelligence operations are in line with the constitution, national security policy and legislation. Parliament also approves the budget of intelligence services and can play a strong role in scrutinizing expenditure.

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

Effective parliamentary oversight ensures a bridge between intelligence and the public and brings benefits to all: intelligence community, parliament itself and most importantly, the citizens.

1. When intelligence services are held accountable for fulfilling their legal mandate, their legitimacy and their effectiveness are bolstered. Oversight protects intelligence services from political abuse and can help create well-resourced, meritocratic and non-discriminatory workplaces for intelligence professionals. Enhanced accountability of intelligence services improves the public trust in the government.
2. Effective parliamentary involvement in intelligence oversight, that leaves behind political differences and focuses on national interests, helps parliament build up its credibility as a democratic institution and enhances the respect and trust it receives from both the intelligence community and the public.
3. Effective oversight protects the rights and liberties of citizens and ensures that proper safeguards are in place to prevent abuse and misuse of power. Oversight is crucial for the rule of law, the respect of human rights, and for ensuring taxpayers' money is spent efficiently and economically.

› WHY IS INTELLIGENCE OVERSIGHT IMPORTANT?

Intelligence and security services play a vital role in maintaining the security of the state. Public and open debates on their purpose and power represent a pressure for improving professionalism and efficiency. Without control and oversight ensuring that intelligence services serve national interests and work within the limits established by the Constitution and law, the services may become crisis generators instead of security providers.

Intelligence work infringes human rights; the more numerous are the eyes that monitor these infringements and the voices who ask that they be kept to a minimum, the better.

Security is a public good for which the citizens have to pay. Intelligence and security agencies spend public money and should be accountable to taxpayers.

There is an important public education function to be performed through oversight; this may indirectly build community support for the important work of intelligence and security agencies

The intelligence and security services` need for public acceptability is higher in countries where former autocratic regimes used security services for their own purposes in the past; the services are prone to public suspicion, lack of confidence and attacks on their legitimacy. Oversight helps the services establish their public credibility and redefine their place in a democratic society.

1.2 THE MAIN CHALLENGES IN THE DEMOCRATIC GOVERNANCE OF SECURITY SECTOR

Intelligence oversight is just one piece in the challenging and complex mechanisms put in place in modern states in order to ensure the democratic governance of the security sector, which is composed of all the structures, institutions and personnel responsible for security provision, management and oversight at national and local levels.

The national security system has unique features entailed by its central role in exercising the state legitimate monopoly in the use of force. It accumulates much power and many aspects of its work are covered by secrecy. Still, security sector shares many common features with other public services and should meet similar (if not the same) standards of efficiency, fairness and responsibility as other (public) services. In the absence of proper control and oversight mechanisms, intelligence and security services can easily be drawn into unlawful activities, inefficiency, abuse of power or can be used for political purposes.

The good governance of security sector reflects the state's responsibility to provide efficient and effective security, while ensuring the accountability of security services and their compliance with the law and human rights standards.

› COMMON FEATURES OF EFFECTIVE AND ACCOUNTABLE SECURITY SYSTEMS:

a) **The legal and/or constitutional framework** provides for legitimate and accountable use of force in line with globally accepted norms and standards for human rights, including mechanisms for sanctioning the use of force and identifying the roles and responsibilities of different stakeholders;

b) **An institutionalized system of leadership and management** is put in place, including mechanisms for guidance and oversight of security by authorities and institutions, systems for financial management and overview, as well as human rights' protection;

c) **Capacities:** structures, staff, equipment and resources towards ensuring efficient security;

d) **Mechanisms for interaction** among security stakeholders: establishing transparent modalities for coordination and cooperation among different stakeholders, based on their constitutional/legal roles and responsibilities;

e) **Culture of service:** promoting unity, integrity, discipline, impartiality and respect of human rights among security stakeholders, and shaping the way in which they carry out individual tasks.

As the institution representing the citizens and the holder of the legislative power, parliaments are entrusted with the control and oversight of the executive in all areas of government, including the security sector. Parliaments oversee the mandate, powers, organization, operations and financing of the all institutions within the security system. Because of the complexity, political nature and the secrecy characterizing the work of security institutions, it is paramount for the parliament to have sufficient legal powers, ability and willingness for an efficient oversight. The main goal of parliamentary oversight is to ensure a balance between the society and the security policy in realizing the objectives, policies and procedures of institutions within

the security system, which often intrude in the civil freedoms and rights guaranteed by the Constitution.

The democratic accountability of security sector incorporates several fundamental principles: transparency, legality, accountability, participation and publicity. Participation should be carefully considered and remembered by any parliament, because, as powerful and effective as it might be, a parliament will never be able to ensure democratic accountability on its own. Parliamentary oversight is only one of five distinct levels of security sector accountability, that ought to be complementary and reinforcing each other, the other levels being internal control by the security services themselves, executive control by ministers and other politically appointed managers, judicial review and external oversight by the media and civil society.

Further on, there are a few preconditions that make democratic and parliamentary oversight possible and functional[2]:

- The state should be the only stakeholder in the society to have legitimate monopoly in force, thus making the security system accountable before the legitimate democratic authorities;
- The parliament is the sovereign and holds the executive responsible for the development and realization of the security policy;
- The parliament has the constitutional role to approve and control the budget allocated for the needs of the security system;
- The principles of good governance, compliance with human rights, and rule of law are applied in all government sectors, and accordingly in the security system;
- The staff of the security system personally reports before the courts regarding violations of national and international laws;
- The security system should be politically neutral.

WHAT ARE THE TYPICAL CHALLENGES IN THE DEMOCRATIC OVERSIGHT OF INTELLIGENCE?

***Secrecy**:* management, control and oversight of a large governmental bureaucracy is more complex when there is a need for secrecy. Independent but complementary oversight institutions with clear mandates for access to information can help overcome this problem.

***Discretion**:* intelligence professionals commonly have discretionary authority to make independent decisions during their work. Effective oversight is time-consuming and difficult.

Political will: due to the level of secrecy in intelligence services, many aspects related with intelligence oversight cannot be publicly discussed, therefore are not necessarily useful for winning citizens attention and votes. Thus, elected representative 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

2 Oliver Bakreski (2010): Role of parliament in security sector, *Contemporary Macedonian Defense*, no. 19, Ministry of Defense of Republic of Macedonia, Skopje, p. 43

analysis does not over- or under-estimate the severity of a threat to national security.

***International scope**:* international intelligence cooperation extends the powers and activities of national intelligence services beyond the reach of national systems of control and oversight. Oversight powers do not reach beyond national jurisdiction but defining the scope and nature of international cooperation can prevent abuses and bolster the credibility of national intelligence services.

***Technology**:* technologies used in intelligence work advance faster than the mandates and powers for their oversight and control, leading to gaps in accountability. Technical experts can provide oversight authorities with key information, while legislatures need to ensure that legal frameworks keep abreast of such changes.

2

THE MACEDONIAN STRATEGIC AND LEGISLATIVE FRAMEWORKS FOR INTELLIGENCE OVERSIGHT

Governments and parliaments need high-quality intelligence in order to make appropriate decisions on national security in a number of areas, from setting the size and budget of specific security forces to authorising the use of force. In addition to being consumers of intelligence, parliaments debate, negotiate and enact the strategic and legal documents that create the environment in which intelligence services operate and define the **legal authority** parliament and its committees have when engaging in oversight.

This section will review the current strategic and legal framework in the Republic of North Macedonia, providing a brief appraisal of the main legal provisions regulating intelligence work, the organisation of different services and the kinds of information publicly available on intelligence powers, methods and means. Parliamentary oversight involves the duty and responsibility to ensure the clarity and comprehensiveness of the strategic and legal frameworks. The major legislative reform undertaken by Macedonian authorities in 2018-19 prove that potential shortcomings in strategic planning and in legislation are carefully considered by those responsible, so that intelligence governance and accountability are continuously improved.

2.1 THE STRATEGIC FRAMEWORK FOR NATIONAL SECURITY

In a democracy, it is the society, not the intelligence services, who defines national interest and what constitutes a threat to national security. This is usually a lengthy process which results in the formation of national security strategy, policy and legislation. Thus, the Parliament's involvement in the debate and often in the approval of strategic planning documents is the starting point for oversight. The Parliament should pay particular attention to two aspects of the strategic framework:

- The strategic planning documents must meet the values and principles enshrined in the constitution;
- The powers of the intelligence services should extend only to the objectives, mandates, priorities and limits set out in the strategic security framework.

The strategic framework for national security affects people's lives, values and welfare and it should not be left to the judgement of the executive alone. The strategic security framework should be centred on the life, values and well-being of people, integrating perspectives from, and being accessible to diverse communities comprising different ages, genders, religions, ethnicities, sexual orientations and other minorities. A strategic framework which is not comprehensive, updated and accessible to the public can be considered a weakness for democratic governance, hampering a coherent and strategic approach to security sector oversight.

Medium and long-term strategic documents such as the *national security policy* provide an integrated framework for describing how a country provides security for the state and its citizens. These documents can also be called *plan, strategy, white paper*, *concept* or *doctrine*. They define security needs and priorities, identify institutions responsible for different aspects of security and give them policy guidance as well as an indication of the resources and means to be used in order to achieve the expected security objectives. Sometimes there are both public and classified versions of such documents, in order to balance the need for transparency and secrecy. Responsibilities for drafting, adopting and updating such documents should be

clarified by law and parliamentary committees should exercise pressure on the government to observe the timelines of this process.

› WHAT ARE SOME KEY STRATEGIC QUESTIONS IN INTELLIGENCE OVERSIGHT?

- Are intelligence officials working within the strategic framework established by government and approved by parliament?
- Do intelligence services have sufficient legal powers, budget and personnel to fulfil their mandate?
- What systemic problems have arisen within the security sector from an intelligence activity or process?
- Have political leaders misused intelligence services? If so, how can this be prevented?
- Do intelligence professionals provide impartial and objective analysis or is their analysis politicized?

The most comprehensive strategic document for national security in the Republic of North Macedonia is the **National Concept for Security and Defence**[3]. The Concept defines the national interests, provides an analysis of the general security environment (including risks, threats and opportunities), and sets the goals and guidelines for the national security and defence policy. The concept has not been updated since its adoption by Parliament in 2003.

The Concept requests the Government to further develop and adopt an integrated **National Security Strategy** "as soon as possible". This happened in 2008, but the document is not publicly available.

The President adopts a **National Defence Strategy,** prepared by the Ministry of Defence[4]. The latest National Defence Strategy dates from 24 March 2020[5]. The document is not debated or adopted by Parliament.

The **Security Council of the Republic of North Macedonia** assumes a significant place in the functioning of the security system. The Security Council is comprised of: the President of the Republic of North Macedonia, the Speaker of Parliament, the Prime Minister, ministers managing state administration authorities in the fields of security, defence and foreign affairs, and three members appointed by the President. The President also chairs the Security Council. When appointing the three members, the President takes into consideration that the Council's composition appropriately reflects the structure of the country's population. The Security Council's structure and its functions are regulated by the Constitution[6] of the Republic of North Macedonia.

The Council reviews and initiates issues related to the security and defence of the country, formulates and gives proposals to the Parliament and the Government, which then adopt,

3 Art. 17, Law on Defence, Official Gazette of the Republic of Macedonia, no. 42/2001, 05/2003, 58/2006, 110/2008, 51/2011, 151/2011, 215/2015, 42/2020, Decision of the Constitutional Court of Republic of Macedonia U. no. 37/2002 (Official Gazette no. 73/2002) and U. no. 135/2002 and 155/2001 (Official Gazette no. 78/2002)

4 Art. 18, Law on Defence, Official Gazette of the Republic of Macedonia, no. 42/2001, 05/2003, 58/2006, 110/2008, 51/2011, 151/2011, 215/2015, 42/2020, Decision of the Constitutional Court of Republic of Macedonia U. no. 37/2002 (Official Gazette no. 73/2002) and U. no. 135/2002 and 155/2001 (Official Gazette no. 78/2002)

5 Defence Strategy of Republic of North Macedonia, Official Gazette of the Republic of North Macedonia no. 75/2020, adopted on the basis of Article 18 Paragraph 1 Point 1 of the Law on Defence, Official Gazette of the Republic of North Macedonia no. 42/2020

6 Article 86 and Amendment XIII, Constitution of the Republic of North Macedonia, Official Gazette of Republic of Macedonia no. 52/1991

endorse or consider them when executing their functions, especially those related to the country's defence, security and protection.

Although the Security Council has the role of an advisory authority, its composition and the issues it discusses and on which it builds positions, opinions and adopts conclusions, make it an exceptionally important authority. It plays a crucial role in the creation of the state's defence and security policies, and in the general functioning of the defence and protection systems.

Reforms implemented in 2017-2020 in the security-intelligence sector have created an increased need for coordination, i.e. the establishment of a mechanism for timely and comprehensive management of security risks and for grading the level of threats on national security. A **Council for Coordination of the Security-Intelligence Community** has been established for the purpose of coordinating the security-intelligence community.

The Council for Coordination of the Security-Intelligence Community is comprised of: the **Prime Minister of the Republic of North Macedonia,** the Deputy PM for the Ohrid Framework Agreement Implementation and Political System, **the Minister of Interior, the Minister of Defence, the Minister of Foreign Affairs, the Minister of Finance, the director of the National Security Agency, the director of the Intelligence Agency; and the head of the competent organizational unit for military security and intelligence within the Ministry of Defence[7].** The Council is set to contribute in overcoming weaknesses and shortcomings in the functioning of security-intelligence services, ensuring a high degree of efficiency and performance in their operations.

› INCREASED COOPERATION AND COORDINATION OF SECURITY-INTELLIGENCE AGENCIES AIMS TO ACHIEVE[8]:

- Coordinated operations of security-intelligence services in the Republic of North Macedonia;
- Joint assessment for areas in the interest of the beneficiaries and joint framework regarding security priorities;
- Briefing the President, the Speaker of Parliament and the Prime Minister, based on assessment incorporating information from all relevant sources, collected through most efficient use of resources;
- Integrated security policy.

A separate Office[9] is established within the Council for coordination, tasked with unifying and assessing the objectivity and relevance of submitted intelligence reports, analyses, assessments and other information on threats and risks to national security. The Office issues recommendations for national security and makes assessments on the level of threats and risks to national security. The Office is managed by a Secretary, who is appointed and dismissed by the Government of the Republic of North Macedonia for a period of two years.

Besides the strategic documents that are specific for security and defence field, important information is laid down in the Programme of Government which sets out the medium-term political framework for future reforms and the basis upon which legislation, yearly budgets and

7 Law on Coordination of Security-Intelligence Community in Republic of North Macedonia, Official Gazette of the Republic of North Macedonia no. 108/2019

8 Ibid, Article 4 Paragraph 2

9 Ibid, Article 12

activity plans will be elaborated by the executive. The document is presented to the Parliament for debate and endorsement, and once approved it should become the main point of reference for assessing government performance. Parliamentary oversight activities should always take as their starting point concrete measures, reforms, policies and commitments undertaken in the Programme of Government. The programme of the Government 2017-2020 had defined the reform of the Directorate for Security and Counterintelligence (UBK) as a key priority, which was already implemented in 2018, following Priebe recommendations and European best practice. Moreover, the Government committed to fully support parliamentary oversight over the service[10].

Based on the Programme of Government, each ministry of the Macedonian Government develops a 3-year **strategic plan** which is updated annually. These documents review the results achieved by the ministry in the previous year and establish the mission, vision, working principles and priorities for the 3-year period that follows. The strategic plans of the Ministry of Interior and the Ministry of Defence[11] provide information on issues such as: planned development programmes, forthcoming projects, strategies to be adopted, human resource development etc. But they do not make reference to the activity of their respective intelligence departments; neither do they explain how intelligence activities integrate in the overall strategy of the ministry. However, this information should be made available to parliamentary committees upon their request. The ministries can be asked to develop a public version of the strategic plan, and a classified one (covering intelligence departments), that can be made available to the relevant committees.

2.2 THE LEGAL FRAMEWORK FOR INTELLIGENCE SERVICES

International human rights standards and the rule of law[12] require that intelligence services' mandate and powers are defined in legislation. The law has to be clear, foreseeable and accessible. Safeguards against arbitrary action should be well grounded in legislation, to counterbalance secrecy and guarantee against discrimination, human rights violations and lack of accountability. The government may issue secondary or subsidiary regulations – such as decrees, ministerial orders or instructions – that are not made available to the public. However, these should cover only specific information that could jeopardise the work of intelligence services and/or national security if made public (such as operational methods and the use of particular devices or technologies). Regulations that are not made public must still comply with existing public laws and the constitution.

› WHAT ARE THE CURRENT EUROPEAN STANDARDS ON THE QUALITY OF THE LAW REGULATING INTELLIGENCE?

UN Human Rights Council recommends that all intelligence services are constituted through, and operate under, publicly available laws that comply with the Constitution and international human rights law. Intelligence services can only undertake or be

10 See page 27 of the document: Program of Government_2017-2020

11 MoI addopted a three year Strategic Plan 2020-2022 on 10.02.2020. MoD has addopted a Defence Capabilities Development Plan for 2019-2028. The documents are available online in Macedonian: https://mvr.gov.mk/Upload/Editor_Upload/STRATESKI%20PLAN%202020-2022(1).pdf http://www.mod.gov.mk/wp-content/uploads/2019/10/%D0%94%D0%9F%D0%A0%D0%9E%D0%A1-2019-2028-finalna-verzija.pdf

12 The principle whereby all members of a society (including those in government) are considered equally subject to publicly disclosed legal codes and processes.

instructed to undertake activities that are prescribed by and in accordance with national law. The use of subsidiary regulations that are not publicly available is strictly limited, and such regulations are both authorized by and remain within the parameters of publicly available laws. Regulations that are not made public do not serve as the basis for any activities that restrict human rights. *(UNHRC Report of the Special Rapporteur Martin Scheinin, UN good practices on mandate and legal basis, Practice 4, 2010)*

The European Court of Human Rights (ECtHR) has held that national legal frameworks must be clear, accessible and foreseeable. It obliges Member States to enshrine minimum safeguards in law, such as specifying the nature of offences that may lead to interception orders and defining the categories of people who may be put under surveillance. (*see for example Roman Zakharov v. Russia, No. 47143/06, 4 December 2015, paras. 227-231)*

European Union Agency for Fundamental Rights (FRA) recommends that EU Member States should have clear, specific and comprehensive intelligence laws. National legal frameworks should be as detailed as possible on intelligence services' mandates and powers, and on the surveillance measures they can use. Fundamental rights safeguards should feature prominently in intelligence laws, with privacy and data protection guarantees for collecting, retaining, disseminating and accessing data. (*FRA, Surveillance by Intelligence Services, 2017*)

The Court of Justice of the EU states that national legislation must lay down clear and precise rules governing the scope and application of a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. Legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary. (*CJEU, Joined Cases C-203/15 and C-698/15, Tele2 Sverige and Watson v. Home Secretary, 21 December 2016, para. 109)*

The mission of intelligence services is to protect national security and to prevent threats to national security. Therefore, how national legislation defines the **concept of national security** and the **threats to national security** determines the legal foundations of intelligence work.

But this is an area that lacks clear international standards. The definition of national security is considered to be a matter of national sovereignty; how national security and threats to national security are defined is decided by the discretion of national parliaments.

- The **European Union** lacks competency to legislate in the area of national security and the European Court of Justice does not have jurisdiction over cases that involve measures conducted by national authorities to safeguard the internal security of EU members.
- National security is mentioned in paragraph 2 of Articles 8, 10 and 11 of the **European Convention on Human Rights (ECHR)** as the first of the "legitimate aims" enabling states to exercise exceptional powers which may limit the protection normally afforded to fundamental rights.
- **The European Court for Human Rights (ECtHR)** case law in the area of national security is growing in recent years, becoming the main guidance for defining the right balance between the imperatives of national security and the respect for human rights in national

regulatory frameworks and practice. The term remains vaguely defined, ECtHR giving it a degree of flexibility, reflected by the "margin of appreciation" which states have in this sphere. However, European case-law has made it possible to assign some substance to the concept of national security. The term "margin of appreciation" refers to the space for manoeuvre that the Strasbourg organs are willing to grant national authorities, in fulfilling their obligations under the European Convention on Human Rights.[13] It most definitely includes **the protection of state security and constitutional democracy from espionage, terrorism, support for terrorism, separatism and incitement to breach military discipline**[14].

The term "national security" was defined for the first time in the Macedonian Law on Coordination of the Security-Intelligence Community, adopted in 2019. According to this law, "national security is a state of social, economic and political stability that is necessary for the survival and development of the country as a sovereign, democratic, independent and social state, as well as for the maintenance of the constitutional order, for the state of continual realization of the fundamental rights and freedoms of the person and the citizen in compliance with the Constitution" [15].

This legal definition is aligned with the general principles enunciated in different international documents. National security and defence interests of North Macedonia stem directly from the fundamental values established in the Constitution:

- Maintaining the independence, sovereignty and territorial integrity and the country's unitary character as an essential framework for preservation and enhancement of the national identity and free fostering and expressing of the ethnic and cultural identity of all citizens;
- Protecting and promoting peace and security, life and health, property and personal security of citizens;
- Maintaining and promoting the state's democratic values;
- Human rights and freedoms;
- Maintaining and promoting a firm and functional multi-ethnic democracy;
- Political-defence integration in NATO, political, economic and security integration in the European Union, and active participation in other forms of international cooperation.

2.2.1 The Security intelligence community

The Macedonian security-intelligence community includes the following security-intelligence services: the Intelligence Agency (IA), the National Security Agency (NSA), and the intelligence unit for military security and intelligence within the Ministry of Defence, i.e. the Military Service for Security and Intelligence (MSSI).

› WHAT KIND OF INTELLIGENCE SERVICES AND FUNCTIONS ARE THERE?

External or Foreign Intelligence - collect, analyse and produce intelligence relevant to the external security of the state and warn of impending external threats;

13 Steven Greer (2000): The Margin of Appreciation: Interpretation and Discretion under the European Convention on Human Rights, Council of Europe, p. 5

14 National Security and European case-law, ECtHR, Research Division, 2013, p. 5 https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf

15 Law on Coordination of Security-Intelligence Community in Republic of North Macedonia, Official Gazette of the Republic of North Macedonia no. 108/2019

Internal or Domestic Intelligence (often called security services) - collect and analyse data relevant to the internal security of the state and the maintenance of public order and safety.

Criminal Intelligence - produce intelligence on organised crime, corruption and criminal activities to aid in law enforcement.

Counter-intelligence – detect and disrupt espionage conducted by foreign intelligence services that is directed against the interests of the state and its population.

Military or Defence Intelligence - generate intelligence relevant for defence planning, the protection of armed forces personnel and bases and the support of military operations; they are part of the armed forces and their mandates are more limited than those of civilian services

Specialised national centres - focus on particular issues such as counterterrorism, fighting drugs trafficking, cyber defence, protection of dignitaries, financial intelligence etc.

2.2.1.1 Intelligence Agency (IA)

The Intelligence Agency (IA) was established by law[16] in 1995 as an independent state institution. The Law stipulates that "*the Agency is responsible for collecting data and information of relevance for security and defence of the Republic of North Macedonia and the economic, political and other interests of the state. The IA carries out analysis and research of the collected information and must inform the President, the Government and other state institutions for issues within their areas of responsibility.*"[17]

As foreign intelligence agency, IA is of great importance for the national security system and the implementation of the state`s security policy. IA develops mechanisms for prevention, anticipation, early warning and estimation of risks and threats to national security. Its powers and responsibilities include[18]:

- Early warning, assessment and predictions on trends and possible security risks
- Collection and analysis of data and information of significance for security and defence, economic, political and other vital interests of the state;
- Collection of data and information for prevention of international terrorism and transnational organized crime;
- Cooperation with other national authorities and international stakeholders for the purpose of timely exchange of data, reports and information.

The Director of the Agency is appointed for a four-year term by the President, who can also dismiss him. Information about the number of employees and total budget and of the IA, without further breakdown among budget lines, are available online on the IA website[19]. The IA is organised in six directorates[20]:

- Hybrid Strategies and Threats Intelligence;
- Terrorism and Other Asymmetric Threats Intelligence;
- Technical Intelligence;

16 Law on Intelligence Agency, Official Gazette of the Republic of Macedonia no. 19/1995

17 Art. 2, Law on Intelligence Agency, Official Gazette of the Republic of Macedonia no. 19/1995

18 https://ia.gov.mk/eng/celinadleznosti_en.html

19 The overall budget of IA for 2019 is 234 650 119 denars or approximately 3.8 million Euros. The Agency has 254 employees.

20 See more in https://ia.gov.mk/eng/organizacija_en.html

- Security;
- General Affairs and Logistics.

In doing its job, the Intelligence Agency establishes cooperation with other national authorities and international stakeholders for the purpose of timely exchange of data, reports and information.

The work and the organisation of the IA are well founded in legislation, important information about the institution being available publicly. There are however areas of possible improvement that should be followed by oversight committees, to make sure accountability is ensured through effective internal control mechanisms and well-developed secondary legislation.

- The law on IA could be more specific regarding the means and methods of operation used. Those are supposed to be defined by the Government, while their use is to be decided upon at the discretion of the Director.[21]
- Parliament has no competences regarding the appointment of the Director. Parliamentary oversight is proscribed in general terms, in the statutory law: "the director is charged with enabling insight and providing all information and data in the scope of the committee's operations"[22].
- The IA employees working in assigned special workplaces do possess and carry weapons, ammunition and other prescribed equipment. Still, they do not have military status.
- The IA law has not been amended since its adoption in 1995[23], leaving important discretionary powers to the Director to regulate any remaining issues with secondary legislation. This might include roles and responsibilities of employees, employment procedures, internal control mechanisms etc.
- IA is not subject to communications interception legislation, however they may apply interception of communication in radio frequencies spectrum.

› WHAT SHOULD BE DEFINED BY THE LEGAL FRAMEWORK?

- Intelligence services' mandates, including specific areas of responsibility and a comprehensive list of their tasks; limits to their mandate, such as the prohibition on promoting or protecting special interests of any particular political, religious, ethnic or other group;
- Permissible and non-permissible methods and activities and the restrictions imposed on their use, especially any method and activity that may interfere with human rights;
- Organizational structures and responsibilities of divisions;
- Modalities for cooperation with other governmental and non-governmental bodies, including exchange of information and joint operations;
- Control and oversight mechanisms by which the services will be held accountable, including the internal, executive, judicial and legislative control, as well as special independent bodies;
- Means for legal recourse in instances of complaint, abuse or violation of rights.

21 Law on the IA: articles 2, 13 and 16 may be interpreted as a carte blanche over methods; this would fall foul of ECHR and make oversight challenging. IA is also not within the oversight structure of the 2018 Law on Interception of Communications.

22 Art 11, Law on Intelligence Agency, Official Gazette of the Republic of Macedonia no. 19/1995

23 A new draft law on IA entered the legislative procedure in February 2020, but the Parliament dissolved immediately after.

2.2.1.2 National Security Agency (NSA)

The National Security Agency (NSA) was established in 2019[24] as the main domestic intelligence service of North Macedonia. It replaced the Administration for Security and Counterintelligence[25] which was dissolved. Unlike its predecessor, NSA is not a part of the Ministry of Interior, but an independent legal entity, and it holds no police powers. Its main tasks are counterintelligence, anti-terrorism and the protection of the constitutional order.

The creation of a separate and completely independent domestic intelligence agency, deprived of police powers, was an important step in North Macedonia`s alignment to European standards and good practices, and in the country's preparation for full NATO membership (which was accomplished in March 2020) and accession into the European Union.

The agency is managed by a director who is appointed and dismissed by the Government upon a proposal by the Prime Minister, having a 5-year term and the right for re-election.

The NSA's jurisdiction is to collect, process, analyse, assess, exchange, keep and protect data and information, with the aim of detecting and preventing activities that are related to security threats and risks to national security of the state:

- Espionage,
- Terrorism and its financing,
- Violent extremism,
- All forms of serious and organized criminal activities aimed against the state,
- Crimes against humanity and international law,
- Unlawful production and proliferation of weapons of mass destruction or their components, materials and devices required for their manufacturing,
- Violation of the security of holders of high offices and facilities of strategic significance for the state,
- Other activities related to security threats and risks to national security of the state.

The organization of the NSA is based on a functional and territorial principles, at central and regional level, determined by a decree adopted by the Government. On the central level, NSA is organized in four main directorates: Directorate for Operations, Directorate for Analytics, Directorate for Operational Technique and Directorate for Logistics[26].

On national security issues, NSA reports to the President, the Speaker of Parliament, the Prime Minister, the Council for Coordination of the Security-Intelligence Community, as well as to other stakeholders depending on the report's subject. If collected data and information points to the existence of grounds for suspicion that an ex officio crime is being prepared, organized or committed, NSA immediately informs the competent public prosecutor's office.

NSA uses different methods and sources for information collection: open (public) sources; individuals; official data and information from state authorities; public enterprises; official records, collections and data registers. A distinctive legal power of NSA is the use of intrusive methods for information collection: interception of communications; surveillance and recording of telephone and other electronic communications, secret associates and undercover agents, monitoring postal and other deliveries.

24 Law on National Security Agency, Official Gazette of the Republic of North Macedonia no. 108/2019

25 commonly referred to by the acronym UBK in Macedonian

26 http://www.anb.gov.mk/en/zaAgen-en.html

The Law on Interception of Communications[27] adopted in 2018 makes the necessary distinction between

(1) the interception of communications as a special investigative measure, used by law enforcement in order to collect evidence in criminal proceedings, and

(2) the implementation of measures for interception of communications for the purpose of protecting the interests of security and defence of the state, used by NSA in prevention and identification of possible threats. NSA needs to obtain authorisation from the Supreme Court in order to be able to legally collect information using such measures.

According to the law, there are situations when NSA may use special technical devices and equipment without the Operational Technical Agency and operators acting as intermediaries. The measure for interception and recording of telephone and other electronic communications, determined by the Law on Interception of Communications (Art. 34), can be performed by NSA only when it is technically impossible to monitor and record the content of the communication without the use of special technical devices and equipment. (Law on NSA, Art. 26).

The statutory law of NSA has a special chapter on the transparency of the Agency's operations. Article 64 of the law, "Informing and communicating with the public", stipulates that the Agency on its website[28] will publish "relevant regulations of the importance of the work, organizational structure of the Agency, and an annual work report". The Agency commits to publish surveys and brochures from the scope of its work and public job advertisements on its website.

2.2.1.3 Military Service for Security and Intelligence (MSSI)

The Military Service for Security and Intelligence (MSSI) is an integral part of the Ministry of Defence (MoD) and the Army of the Republic of North Macedonia (ARNM) . The Law of Defence[29] does not refer to it as a separate organizational unit. Nevertheless, it defines intelligence and counterintelligence for defence, which are the two inseparable pillars of the MSSI. They include:

- detection and prevention of intelligence and other subversive activity of foreign military intelligence and counterintelligence services, carried out in the country or abroad, which is aimed at the defence of the Republic;
- detection and prevention of all forms of terrorist activity aimed at the defence of the Republic;
- conducting counter-intelligence protection of tasks and plans, documents, material and technical means, areas, zones and objects of defence interest.

The MSSI has two components:

1. The **Sector-Service for Military Security and Intelligence** within the MoD. The Sector-Service has nine units, including: Unit for planning and general matters, Support unit, Unit for CCIRM[30], Intelligence Unit 1, Intelligence Unit 2, Counterintelligence Unit, Unit for Security, Unit for Physical Security and Unit for Analytics[31].

2. Sections within the ARNM: **J-2, S-2, A-2.** These sections are double hatted: by command functions under the General Staff of ARNM; and by professional functions under the Head of Sector-Service for Military Security and Intelligence.

27 Law on Interception of Communications, Official Gazette of the Republic of North Macedonia no. 71/2018

28 www.anb.gov.mk

29 Art. 133, Law on Defence, Official Gazette of the Republic of Macedonia, no. 42/2001, 05/2003, 58/2006, 110/2008, 51/2011, 151/2011, 215/2015, 42/2020, Decision of the Constitutional Court of Republic of Macedonia U. no. 37/2002 (Official Gazette no. 73/2002) and U. no. 135/2002 and 155/2001 (Official Gazette no. 78/2002)

30 Collection, Coordination, Intelligence Requirements Management (CCIRM)

31 http://morm.gov.mk/wp-content/uploads/2017/06/Organogram-juni-2017.pdf

How MSSI conducts its work is regulated by by-law[32] based on Article 136 of the Law on Defence. MSSI conducts background checks for security vetting of personnel within the defence establishment. Authorized persons from the MSSI have the right to collect data, information and notification[33].

There is no publicly available information on the MSSI staff, and their budget is incorporated in the budget of MoD. MSSI does not have a separate budget and for all financial purposes it is treated as part of MoD budget.

The director of MSSI is appointed by the Minister of Defence.

MSSI cooperates and exchanges information with military intelligence and counterintelligence services of partner-countries and coordinates with NATO's intelligence systems. Staff of MSSI is deployed in international military peacekeeping missions North Macedonia takes part in.

2.2.2 Other institutions holding authority to use intrusive methods

In addition to the institutions deriving their mandate from the Security Intelligence Community Law, a few other bodies within the Macedonian Government play a non-negligible role in the intelligence sector, namely the Public Security Bureau, the Financial Police Office, the Customs Administration, the Centre for Electronic Surveillance and the Operational-Technical Agency. Notably for the purposes of criminal procedures, these authorities have some intelligence prerogatives, through internal units for criminalistic intelligence and analysis, or sectors for control and investigations. Their intelligence functions give them the power to collect information with intrusive methods, among others, with interception of communications. While they are not always bound to present specific reports for their intelligence work, they form a part of the Macedonian security system, and are subject to parliamentary oversight conducted by the Committee for Defence and Security and the Committee on Oversight of the Implementation of Measures for Interception of Communications.

2.2.2.1 Public Security Bureau (PSB)

The Public Security Bureau is an authority within the Ministry of Interior in charge of police affairs, which structure and jurisdiction are regulated by the Law on Police[34]. PSB is part of the judiciary police and according to LIC is one of the authorized bodies for communications interception for criminal investigation purposes; they also have legal authority to use undercover agents. PSB director is appointed and dismissed by the Government at the proposal of the Minister of Interior, for a 4-year term.

The PSB is mainly responsible for:

- the conceptual planning, monitoring and analysis of the state of security and the causes for crime and threat to public security;
- general and expert oversight and control of the police's organizational units;

32 Rulebook on Operations in Intelligence, Counterintelligence and Prevention and Detection of Crimes in Defense, Official Gazette of the Republic of North Macedonia no. 40/2003

33 MSSI employees (both MoD unit and Army sections) are authorized official persons granted with authorizations defined in Art. 133, 134, 136 of the Law on Defence. The Law on Interception of Communications Art. 4, para. 1. point 7 identifies as authorized authorities for the implementation of the measures for interception of communications for the purpose of protection of the security and defense interests of the country: the National Security Agency and the Ministry of Defense - Military Service for Security and Intelligence; and the Centre for Electronic Reconnaissance of the Army as authorized authority for the frequency specter of radio waves of high, very high and ultra high frequencies (HF, VHF and UHF)

34 Art. 15, Law on Police, Official Gazette of the Republic of Macedonia no. 114/2006, 06/2009, 145/2012, 41/2014, 33/2015, 31/2016, 106/2016, 120/2016, 21/2018, 64/2018 and Decision of the Constitutional Court of Republic of Macedonia, Official Gazzete of Republic of Macedonia no. 148/2008

- processing personal data under conditions and in a way established by the law on police and a specific law;
- implementation of ratified international agreements on police cooperation and other international acts in the police's jurisdiction;
- the preparedness of the police to act and work in conditions of complex state of security.

The internal structure of the PSB is based on linear and territorial principle. The main organizational units established within the PSB are the following:

- Police Affairs Department is responsible for the daily police work in the area of public order and peace, prevention, and police activities related to complex states of security;
- Criminal Police Department coordinates measures and activities conducted by organizational units for criminal affairs and regional centres for border affairs, to ensure uniform proceedings by operational police services in the field.
- Criminal Intelligence and Analysis Department collects, processes and analyses data and information, drafts analytical products and reports, and disseminates them to the organizational units across Public Security Bureau.
- Border Affairs and Migrations Department is responsible for daily police work in the field of border affairs, police activities related to cross-border crime and migrations, and affairs related to foreigners and readmission.
- Traffic Affairs Department is responsible for traffic, issuing and revoking the license of a driver-instructors, the inspection of the manner of implementing drivers' exams, exams for inspection of competencies of driver-instructor;
- Common Affairs and Human Resource Management Department is responsible human resource management, legal and financial affairs, personal data protection, staff development, representation of communities and gender equality.

PBS has important responsibilities in the internal control of police, which are met by the following structures:

- The Sector for Internal Control, Professional Standards and Criminalistic Investigations performs internal control in cases of possible misuses of police powers.
- Special ad-hoc committees formed by the Director conduct general and expert oversight and control of police organizational units[35].
- Eight Sectors for internal affairs are established on national territory for the purpose of conducting police affairs. They are set up according to the size of the area, population size, number of crimes and misdemeanours, and significance of roads and geographic position of municipalities.
- Four regional centres for border affairs are established for conducting police affairs relating to border inspections and border supervision[36].

2.2.2.2 Financial Police Office (FPO)

The role of the Financial Police Office is important in the fight against sophisticated forms of organized crime, resulting from the globalization and the swift technology development in countries of transition. FPO is a distinct legal entity within the Ministry of Finance established

35 Rulebook for oversight and control in the Police, Official Gazette of the Republic of Macedonia no. 42/2007 and 14/2017

36 Law on Police and Law on Internal Affairs, as well as on the website of MoI https://mvr.gov.mk/page/organogram

in 2003 through a specific law[37]. It is mandated to protect national financial interests, acting in the field of financial, tax and customs operations, detecting and pursuing complex forms of organized financial crime.

The FPO is managed by a director appointed and dismissed by the Government at the proposal of the Minister of Finance. Its organizational structure incorporates:

- Sector for Criminal Intelligence Analysis,
- Sector for Integrated and Financial Investigations, and
- Sector for Financial, Normative-Legal Affairs and Human Resources.

The FPO is an integral part of the judicial police as a law enforcement authority for crimes in the field of organized financial crime and other crimes prosecuted ex-officio, which result in acquiring illicit property gains of significant value or damaging the national budget.

The FPO carries out detection and criminal investigation of crimes in the field of organized financial crime prosecuted ex-officio, as well as catching and reporting their perpetrators, securing evidence and other measures and activities that can be used for a continual criminal investigation.

Moreover, it collects and analyses data on cash transactions, undertakes pre-investigative and other measures with grounds of suspicion on committed crimes, follows the money trail in order to detect crimes defined by law, as well as insight and review of accounting data and registries in computer systems, in the presence of a responsible person or his proxy. The FPO's role is especially important in conducting forensic computer analysis of temporarily confiscated IT systems and other electronic devices.

2.2.2.3 Customs Administration

The Customs Administration is an authority of the state administration within the Ministry of Finance, having a status of a separate legal entity and established through a specific law[38]. It is managed by a director who is appointed and dismissed by the Government of the Republic of North Macedonia at the proposal of the Minister of Finance, for a 4-year term.

The basic powers of the Customs Administration are:

- Customs oversight and control duties over the entire territory of the Republic of North Macedonia, investigative and intelligence measures towards prevention, detection and investigation of customs violations and crimes;
- Protection of the security and safety of people, animals and plants, protection of objects of historical, artistic and archaeological value, copyrights and other rights, as well as other measures of the trading policy prescribed by law;
- Customs controls after clearing;
- Internal controls and audit in all spheres of customs operations and the overall functioning of the Customs Administration, towards detecting cases of violations of laws and internal regulations, as well as abuse of office by employees;
- Misdemeanour procedures, issuing misdemeanour sanctions for customs, excise and foreign currency misdemeanour, and initiating a procedure on crimes defined by law.

37 Law on Financial Police Office, Official Gazette of the Republic of Macedonia no. 12/2014, 43/2014, 33/2015, 27/2016, 83/2018 and 198/2018

38 Law on Customs Administration, Official Gazette of Republic of Macedonia no. 46/2004, 81/2005, 107/2007, 103/2008, 64/2009, 105/2009, 48/2010, 158/2010, 53/2011, 113/2012, 43/2014, 167/2014, 33/2015, 61/2015, 129/2015 and 23/2016

The Customs Administration carries out its operations through the central office and five customs houses. The central office coordinates and manages customs operations over the entire territory of the country, while customs houses coordinate and manage a specific region. The operations of the Customs Administration are carried out by the following sectors: Sector for Professional Responsibility, Sector for Customs System, Sector for Excise, Sector for Control and Investigation, Sector for Human Resource Management, Sector for Financial Affairs, Sector for Administrative and Technical Affairs, Sector for Legal Affairs and Sector for Information and Communication Technologies.[39]

The Customs Administration has the legal competence to ask for information and assistance from other state authorities and institutions, as well as cooperate with customs administrations of other countries towards preventing customs violations and crimes.

2.2.2.4 Centre for Electronic Reconnaissance (CEI)

The Centre for Electronic Reconnaissance is a unit within the General Staff of the Army of the Republic of North Macedonia. It is managed by a commander appointed by the Chief of the General Staff. CEI collects intelligence data by way of electronic reconnaissance, with the aim of early warning and protection of armed forces. Electronic reconnaissance is especially significant in time of war for collection of information about the enemy. CEI contributes to:

- effective deployment of the armed forces, including in missions outside national territory;
- securing defence facilities;
- obstruction in the electromagnetic spectre;
- electronic protection of forces;
- support of cooperative defence actions during an attack to the country;

The Centre for Electronic Reconnaissance is authorized to intercept communications but only in a relevant radio spectre (HF-High Frequency, VHF-Very High Frequency, and UHF-Ultra High Frequency) that are specific for defence purposes[40].

2.2.3 Operational-Technical Agency (OTA)

In the framework of the reforms of the system for interception of communications, within the wider Security Sector reforms in Republic of North Macedonia, a specific law[41] establishes a new agency with a technical role. The Operational-Technical Agency (OTA) is an independent state authority that ensures a technical link between service operators and competent authorities for the interception of communications, in cases when a court order has approved the interception of communications for the purpose of **criminal investigation** or for the purpose of protecting the interests of security and defence of the country – **national security**. The OTA does not have the technical capabilities to access the content of the intercepted communications. The technical link between the operators and the competent authorities is enabled, only and exclusively, with issued court order for interception of communications.

The OTA is managed by a director, who is appointed and dismissed by the Parliament of the Republic of North Macedonia. The director is elected by a two-thirds majority of vote of the total number of MPs, and by a majority vote of MPs belonging to the non-majority communities, upon

39 http://www.customs.gov.mk/index.php/en/about-us-en/koi-sme-nie/organizacija-mk/sektori-cu-2-mk

40 Art. 4, para. 1. point 7, Law on Interception of Communications, Official Gazette of the Republic of Macedonia no. 71/2018

41 Law on Operational-Technical Agency, Official Gazette of the Republic of Macedonia no. 71/2018

a published call. The director's term is five years without an option for re-election.

The organizational setup of the OTA is regulated by a Rulebook on internal organization, which is classified, and there is no publicly available information.

For the purpose of ensuring technical conditions when linking operators and competent authorities, the OTA is enabling:

- A technical link between operators and the intermediary device (LEIMD)[42] installed in the OTA;
- A technical link between the technical devices (LEIMD and LEMF[43]) installed in the OTA;
- A technical link between the technical device (LEMF) installed in the OTA and the workstations used for the interception of communications installed in the facilities of the competent authorities.

The advantage of the OTA's establishment as a segment of the intelligence sector is the fact that it eliminates the technical possibility for a stand-alone port, interception and recording of telephone and other electronic communications of operators by competent authorities for the purpose of collecting and analysing intelligence information. The OTA is the technical entity, which enables (sends a signal to the workstations) the interception of a certain electronic communication based on a court order. Despite the existence of the OTA, certain services have the option of independent interception of communications without the OTA as intermediary, but only in specific cases[44] and based on a court order.

Intermediary devices for interception of communications owned by the operators are installed in the OTA. This institutional arrangement prevents the concentration of power in only one institution, thus facilitating accountability. The OTA is designed as a 'buffer' between the bodies authorised to use interceptions and the service operators, and thus is performing an expert supervision function within the interceptions system.

A significant portion of the OTA's work is expert oversight of the operators, which is carried out by an Expert Oversight Commission comprised of a chair and two members. The Commission is conducting oversight of the use of technical equipment and electronic communication lines that serve to link the OTA with the operators. Upon executing the oversight, the Commission drafts a report on the work of the operator

The OTA submits an annual report to the Parliament of the Republic of North Macedonia regarding its work, but also additional reports if needed or at the request of the Parliament.

OTA cooperates with national and international state authorities, counterpart organizations from other countries and other international organizations in the field of security, information security and telecommunications.

42 Intermediary device (LEIMD) is an intermediary technical equipment and specific software support that enables the activation of the measure of interception and recording of telephone and other electronic communications

43 Equipment for interception of communications (LEMF) are means for interception of communications to which the content of the intercepted communication and information related to the intercepted communication is transmitted from the technical equipment of operators through OTA to the workstations owned by competent authorities

44 Based on Law on Interception of Communications, Official Gazette of the Republic of Macedonia no. 71/2018

2.3 THE MACEDONIAN INTELLIGENCE OVERSIGHT SYSTEM

There are different levels of control and oversight contributing to intelligence accountability. They are complementary and mutually reinforcing, so deficiencies in one level have the potential to affect the entire system. This section will briefly introduce the main principles and review the most relevant legal provisions underpinning control and oversight in the Republic of North Macedonia.

WHO IS RESPONSIBLE FOR KEEPING THE INTELLIGENCE SECTOR ACCOUNTABLE?

Internal control – by directing officials and mechanisms for internal control and audit. It relies on standing orders, recruitment, training, personnel coordination (including mechanisms for protection of the rights of officers and disciplinary proceedings against individuals).

Executive control – by relevant ministers and executive officials. Based on policies, directives, priorities and accountability before the parliament.

Parliamentary oversight – by relevant oversight committees, based on the Constitution, laws, parliamentary procedures, oversight activities, approval and review of the state budget.

Judicial control (ex-ante and ex-post) – by an independent judiciary. It includes the authorisation of special intrusive powers and trial on alleged violations of the law.

External oversight – by the media and civil society. Based on investigative journalism, independent research, public debate on alternative policies and priorities.

2.3.1 Internal control

Internal management controls day-to-day intelligence activities and ensures that intelligence officers conduct their work effectively in compliance with the relevant national and international law. The values, ethics and legal knowledge of intelligence personnel are of outmost importance.

- Internal management should actively promote a culture of accountability, professionalism, integrity, inclusion, gender equality and respect for diversity, starting with efficient recruitment and training processes. They also coordinate the processes of evaluating performance of personnel. Managers must implement robust selection criteria to ensure they recruit people with appropriate values. They also have to ensure ongoing training is provided, including on human rights issues and on the role of oversight – to foster the awareness and willingness to cooperate with external oversight authorities.
- Directors are appointed for a fixed term of office to protect them from political pressure or changes in government. They can be removed from office only if they breach specific rules.
- Internal inspectors-general assess the legality of service activities and alert managers and the executive to any individual or systemic problems.

Internal control is usually developed in secondary legislation and internal regulations such as procedures for assigning, reporting on and evaluating intelligence activities, or codes of conduct and professional standards. Public information on internal control mechanisms and procedures in Macedonian intelligence services is scarce.

- **The Law on Internal Affairs** envisages a separate organizational unit responsible for assessing legality in the work of the Ministry of Interior (MoI) employees. The Department for Internal Control, Criminal Investigations and Professional Standards acts on information gathered from citizens' complaints, internal documentation and information from MoI employees; it can act upon an order from the MoI. The Department deals mainly with police misconduct.
- **The Ministry of Defence** carries out internal control through inspectors-generals who check whether the employees' performance is in accordance with the relevant laws. The *Sector for Inspection in Defence* conducts oversight on the legality of operations in the Ministry of Defence, the General Staff and the Army; it may also oversee certain affairs in the defence interest, within state authorities, local governments, trading associations, public enterprises, institutions and services, in compliance with the law and Rulebook on oversight in the field of defence. Considering the Long-term Plan for Development of Defence Capabilities 2019-2028, the Ministry of Defence also includes a separate unit - *Sector for Internal Audit.*
- **The Law on Intelligence Agency** has no provisions regulating internal control.
- **The National Security Agency** regulates internal control in its statutory law. It is carried out by a separate organizational unit, whose jurisdiction is prescribed in the law[45].

Parliamentary committees have the responsibility to scrutinize these internal policies, mechanisms and practices. Even if these are based on classified executive orders and internal procedures, oversight committees must get access to these documents.

An important way for the parliament to influence internal control is to have a say in the appointment of service directors. In some countries the executive consults with the opposition parties and/or parliamentary committees prior to appointing directors. Parliament may ask questions about the nominee or invite them for a hearing. This helps prevent the executive from appointing persons who would simply protect or promote their own political interests. It can also promote the integration of more diverse representation and perspectives in the oversight process.

› WHAT IS THE DIFFERENCE BETWEEN *CONTROL* AND *OVERSIGHT*?

Control refers to the power to direct an organization's policies and activities, for example by making rules, codes or policies that determine how an organization functions.

Oversight means verifying whether rules and laws are obeyed, and codes and policies are applied.

Oversight can be undertaken by many different actors and institutions, while control is mainly the responsibility of management and the executive branch.

2.3.2 Executive control

The ultimate authority and legitimacy of intelligence activities relies on parliamentary approval of their powers, mandates and expenditures. But for practical reasons and because of the sensitive nature and the urgency of intelligence work, the effective daily control of intelligence rests within the government.

45 Art. 52-54, Law on National Security Agency, Official Gazette of the Republic of North Macedonia no. 108/2019

The political executive is the main customer, taskmaster, controller and overseer of intelligence services. They establish the overarching policies and priorities for intelligence services, allocate them resources, formulate directives, subsidiary regulations and guidance on different aspects of intelligence work, from information sharing with foreign partners to the use of intrusive measures for information collection. As the main intelligence consumers, the executive must provide guidance about which intelligence products are needed and should give feedback on the intelligence reports received. The absence of such feedback might result in inadequate intelligence products.

The executive must implement an efficient external control of intelligence services. The Government as the central authority of the executive is responsible for national security and therefore must integrate and coordinate capabilities and operational efforts of all institutions within the security sector.

Government structures are equipped to direct and coordinate intelligence services in real time. Responsible ministers need a sufficient degree of control over intelligence services and the right to ask them for information; they also need mechanisms for sanctioning and taking action in cases of legal violations. However, effective executive control does not imply direct managerial responsibility for intelligence operations. There is a need to establish the right balance in the relations between the executive and the intelligence community:

- Too much executive control and influence on the work of intelligence services might lead to the misuse of the services for political interests;
- Not enough executive control creates the risk of misuse of intelligence powers and resources by individuals within the services, for their own personal interests.

› WHICH AUTHORITIES ARE RESPONSIBLE FOR EXECUTIVE CONTROL OF INTELLIGENCE SERVICES?

- Broader ministerial portfolios such as defence, interior or home affairs, justice, for intelligence services organised as integral parts of ministries
- Prime minister (e.g. in UK)
- President (e.g. in Romania)
- Joint authority of a president and a prime minister (e.g. in Croatia and Slovenia)
- Collective body such as the National Security Council (e.g. in Croatia, Romania, Serbia).

In the Republic of North Macedonia, as in all other countries, the executive (including the President of the Republic and the Government) are the main beneficiaries of intelligence work. Services collect and analyse information about threats detected against the state and its population. They provide this information to the Government, enabling it to develop and enforce security policy. Democratic oversight is hindered by the lack of public information as to how executive control is actually implemented.

- The Military intelligence service (MSSI), is responsible to the Minister of Defence.
- The Government appoints and dismisses the director of the National Security Agency (NSA), upon a proposal of the Prime Minister.

- The Intelligence Agency (IA) reports directly to the President, who has the right to appoint and dismiss its Director. The Government has strong competences regarding IA as it prescribes IA methods and means of operation, and is also holding the IA Director to account, but the law does not specify how[46]. The Director, on the other hand, has complete autonomy as to what measures should be used – there is no legal provision for prior checks by Government. Specific methods used in an operation should be classified, but there is no reason why the law should not specify in general terms the methods that are 'prescribed'.

› WHAT ARE SOME SPECIFIC CHALLENGES FOR INTELLIGENCE OVERSIGHT AND CONTROL IN TRANSITIONAL CONTEXTS?

Intelligence services are a crucial element in preserving authoritarian or totalitarian regimes, which means they can pose specific challenges when carried over to new democratic governments:

- Information collected under the former regime can be used for blackmail, extortion or political manipulation;
- Seeking justice for past abuse can create an incentive for powerful interests to stall political transition.
- Impunity for former abuses can undermine new political institutions, especially if personnel from the former regime remain in office.
- Government officials, elected representatives, civil society and media in transition countries may be ill-equipped or unwilling to scrutinize intelligence.
- The lack of a legal framework for democratic oversight and control, fragmentation of services and extensive powers of intelligence services make oversight difficult.
- **Pre-existing laws and regulations may be discriminatory or fail to provide** adequate measures of **redress or access to justice.**

Parliamentary oversight depends on executive control. Overseers need to prevent excessive executive influence leading to improper politicisation of the services, but, on the other hand, they must ensure that the executive has clear legal powers and tools to exert effective control over intelligence work. Ministers can only be called to account for the actions of intelligence services if they have real control over and adequate information about the actions undertaken by the services.

2.3.3 Parliamentary oversight

Intelligence oversight is one of the newest[47] and most challenging areas of parliamentary work. In most democracies today, it is accepted that all state activities should be open for scrutiny and investigation by parliament. Intelligence services are no exception from this rule, even though restrictions and limitations on the information provided to overseers are often applied.

46 Art. 4, Law on Intelligence Agency, Official Gazette of the Republic of Macedonia no. 19/1995

47 Historically, national security, and especially intelligence, have been considered an exclusive field of competence of the executive, whereas the legislative and judicial powers have delayed their interference. It was the 1990s, after the end of the Cold War, when parliamentary oversight of intelligence became a norm and prerequisite for democracy.

WHAT IS THE SCOPE OF INTELLIGENCE OVERSIGHT?

- **Legality** – refers to the conformity with all applicable legal provisions from national primary and secondary legislation, and with the standards deriving from international conventions and soft law (such as decisions of international courts, codes of conduct, resolutions, recommendations, etc.).
- **Effectiveness** – refers to the extent that an intelligence service achieves the specific objectives defined by government policies with respect to national security and public safety
- **Efficiency** – refers to how economically the service uses its financial and human capacities in the execution of its mandate.

TOOLS FOR PARLIAMENTARY OVERSIGHT[48]

Legislative powers

- Setting the legal framework for oversight;
- Influencing government policy and strategy on a broad level, and in security and defence.

Budget control

- Approval of budgetary allocations for each and every security institution;
- Oversight/verification of the respect of the allocated budget;
- Sanction in case of excessive/illegitimate conduct by the executive.

Direct oversight

- Oversight bodies are established and function effectively
  - Parliamentary committee(s);
  - Independent oversight bodies to assist the parliament.
- Involvement in important decisions
  - Prior approval of national participation in military deployments abroad, war, state of emergency, international treaties;
  - A posteriori control of decisions (with a possibility to revoke or modify mandates);
  - Appointment of senior officials (ministers, directors of intelligence, chief of staff);
  - Approval or consultations on important defence procurement
- Access to (classified) information
  - "Obtaining document"/Proactive disclosure
  - Summons/Hearings
  - Information/Consultation
  - Secrecy safeguards
- Investigative powers – parliament can establish inquiry committees with subpoena powers

48 Adapted from Hans Born (2013): Parliamentary oversight of the security sector, European Parliament – OPPD, p. 25. https://www.dcaf.ch/sites/default/files/publications/documents/EP_Parliamentary_Oversight_Security_Sector_2013_BOH.pdf

Specialized standing committees for intelligence oversight have been set up in most European countries, but there is a wide variety of specific arrangements. Essentially there are three approaches in setting up intelligence oversight, evolving towards increased specialisation and organisational complexity.

1) **Defence and security committees.** In some countries, a committee with a broad mandate deals with the legislation and oversight of the entire security sector, including intelligence services and ministerial departments with intelligence activity. This approach enables committee members to develop a comprehensive understanding of the security sector and properly integrate legislative and oversight processes. This is the case in countries like Albania, Montenegro, Moldova, which have a relatively small security sector; however, a decade or two ago, this was the approach used by most democracies and transitioning countries.

2) **Intelligence oversight committees.** A large majority of European parliaments have set up (in addition to defence and security committees) specialised working bodies dealing exclusively with intelligence oversight. They have a narrow, focused oversight mandate, so elected members and staff may make best use of time and resources, develop expertise and engage in sustained oversight activities. Sometimes, the mandate of these committees involves exclusively oversight, and their responsibilities in the legislative process are limited.

3) **Expert bodies external to the Parliament.** An increasing number of states are establishing expert intelligence oversight bodies, in addition to parliamentary committees. The members are senior public figures, prominent members of the civil society, current and former members of the judiciary, or former politicians. They 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. These bodies are usually appointed by the parliament and they report to the parliament and/or the executive. Belgium, Croatia, Denmark, Germany, Greece, Norway, the Netherlands and Sweden are such examples.

The structures created within the Macedonian Parliament and mandated to ensure intelligence accountability illustrate the same evolution towards specialization and institutional complexity in intelligence oversight.

1) A Defence and Security Committee, with general legislative and oversight competency over the whole security sector, is responsible for the oversight of military intelligence within the Ministry of Defence.

2) A specialized intelligence oversight committee supervises the two major services – the National Security Agency and the Intelligence Agency.

3) A third parliamentary committee has a very precise and specialized oversight mandate and monitors the implementation of the intrusive methods for information collection.

4) The Law on Interception of Communications, adopted in April 2018, introduced a new institution in the oversight system: a civilian body external to the parliament (the Citizens Supervision Council), which receives complaints and supervises the legality of interceptions.

Besides these oversight bodies with a special mandate for security and intelligence sector, the Parliament of North Macedonia has set up a standing inquiry committee[49] for protection of

49 Despite its name, the committee doesn't have inquiry powers (subpoena)

human rights and freedoms. The committee considers cases of serious suspicion or findings indicating violation of fundamental rights guaranteed by Constitution.

The legal authority[50] of oversight bodies is the first precondition for effective intelligence oversight. The legal authority of the three Macedonian parliamentary committees rely (1) on general law provisions that regulate parliamentary oversight, and (2) on specific provisions that regulate intelligence oversight.

(1) The legal foundation for parliamentary oversight is defined in the **Constitution** of the Republic of North Macedonia, which states: *"The Parliament carries out political control and oversight of the Government and other public office holders responsible to the Parliament."*[51]

The **Law on Parliament of Republic of North Macedonia** has a separate chapter called "parliamentary oversight" which regulates hearings as the main oversight tool.

The Parliament's Rules of Procedures is the most detailed legal document regulating the rights and obligations of MPs, including the right to information, the use of parliamentary questions and interpellation as tools for oversight, the work with confidential information and the procedure for the election of working bodies.

However, these general provisions do not refer directly to the committees on intelligence oversight. Still, some of them are important tools MPs can use proactively. For instance, in cases where public officials do not show up when invited to committee sessions, or when committees do not convene for any reason, individual MPs may perform oversight by addressing parliamentary questions in the plenary. As the MPs from the oversight committees hold security clearance, they can request a written response in case when the answer contains classified information.

(2) Besides these general provisions that concern the Parliament as a whole, intelligence activities oversight by designated parliamentary committees is briefly prescribed in several laws.

- Article 11 of the Law on the Intelligence Agency states that "the director is responsible to enable insight and to provide all the information and data within the scope of the committee's work".
- Article 60 of the Law on the National Security Agency states that "the director is obliged, at the request of a competent oversight committee, designated by the Parliament, to provide insight on the documentation, provide with data and information on the work of the agency and answer to questions related to the agency's operations".
- Both services are obliged to submit an annual report on their work to the committees. The National Security Agency also submits an annual working programme[52].

The mandate of parliamentary committees i.e. their "scope of work" is defined by a Parliamentary Decision at the beginning of each new legislature.

According to this source of legal authority[53], **the Committee for Oversight of the National Security Agency and the Intelligence Agency** has a strong oversight mandate that incorporates the observance of the law in exercising the authority of the services, respect of human rights, and even the methods and means used by the services, as well as the financial, personnel

50 Annex B provides an overview of relevant excerpts from the law, which give parliamentary committees legislative powers for intelligence oversight.

51 Art. 68, Constitution of the Republic of North Macedonia

52 Art. 60, para. 6, Law on National Security Agency, Official Gazette of the Republic of North Macedonia no. 108/2019

53 Parliamentary decision no. 08-1396/1 of 31 May 2017

and technical facilities. The services are obliged to provide the necessary information for the accomplishment of the committee's oversight mandate.

The **Law on Interception of Communications** (LIC) adopted in April 2018 clarifies and strengthens the Parliament's legislative powers in the oversight of communications' interception. **The Committee on Oversight of the Implementation of Measures for Interception of Communications** mandated with this task is defined by the following features:

Composition. The committee is chaired by a member of the opposition (LIC, Article 38). Giving the opposition a leading role in oversight is considered to be a good practice for establishing the accountability of government activities that happen in secrecy, where abuse and arbitrary use of powers may occur.

Mandate. The committee is mandated to oversee the **legality and effectiveness** (Article 40) in the use of interceptions. The legality is to be assessed by comparing statistical data generated by the service operators, the OTA and other competent authorised bodies on the interceptions implemented (Article 41-3). The committee may perform oversight without prior announcement, if required, and at least once within a three months period, even in absence of majority votes (Article 44). These provisions should help establish a climate of accountability and regular oversight practice. Attention should however be given to several LIC provisions whose further interpretation and implementation are important for clarifying the future scope of oversight:

- security and defence purposes (by NSA and MoD, Article 18), the *efficiency* seems to refer only to interceptions for criminal investigations: the law states that the oversight objective is to be accomplished through the analysis of the report by the Public prosecutor (Article 40(3)).
- To review the effectiveness of interceptions implemented for national security and defence purposes, the committee would need more diverse and complex sources of information.
- According to the letter of the law, oversight seems primarily concerned with ensuring that investigative measures and processes have been implemented properly, and accordingly, focusing on the functional sphere of intelligence, but this does not exclude the possibility of overseeing operational activities and their efficiency.

Access to expertise. The law stipulates (Article 39) that no later than 50 days after its appointment, the committee shall hire two experts for continual technical support. Within 6 months, the committee must create a roster of national and international experts to provide a case-by-case support. The law lists the obligation of other state agencies to provide expert support at the committee's request. These are exceptional measures intended to increase committee expertise and enhance its capability to engage in effective oversight. Insufficient expertise in intelligence affairs is, in every country, one of the biggest challenges in oversight. The LIC provides the committee with several different avenues to solve this problem, and by setting tight deadlines for employing expertise, it compels the committee to act and address this issue.

Access to information. The data the committee has access to in order to fulfil its oversight mandate related to *legality* is specified in LIC Art. 41-3. The committee can check the number of authorisations issued and what types of surveillance was used. If the documentation it has access to contains such specific indications, it may also be able to check for what offences different types of surveillance were used. This type of oversight is important as it can serve to reassure the politicians in the Assembly that surveillance is not overused.

- However, the committee must strive to obtain information that matches its supervision

responsibilities related to the efficiency of interceptions. This means that it should go beyond following "the paper trail" and the comparison of statistical data and develop sufficient fact-finding ability to investigate the conduct and records of relevant agencies.

- Access to classified information (Article 37) notes that members of the oversight body should "own a security certificate with an appropriate level of access to classified information", and such certificate is to be issued within 30 days of the application. Depending on exactly what level of information is to be examined, and especially if this includes operational information, these appear to be unusually short and possibly over-ambitious timescales for ensuring the vetting and approval of security clearances.

Reporting. When oversight activities reveal irregularities, the committee must inform the prosecutor's office, competent (data protection) authorities and, if necessary, the Parliament and the public. The committee can produce special reports when requested by the Parliament. The committee's annual reports are to be made public (Article 45). The law embraces the good practice of stating clear timescales for reports to be published. The committee should submit its annual report to the Parliament by the end of each February at the latest (Article 45(1)), which is quite an ambitious target.

- The law is slightly unclear on when and how the results of investigation and oversight are made public. The committee will inform the public, where appropriate and without disclosing specific data (Article 44). The question of what "appropriate" means here and who decides on it should be clarified in the Committee's Rules of Procedures.
- Another ambitious reporting target is set up in Article 51: The Committee shall notify the Citizens' Oversight Council of the results of any request within 15 days. It is unlikely that this deadline could be met routinely, although it would obviously depend on the staffing resources at the Committee's disposal.

The Law on Interception of Communications refers only to one of the three parliamentary committees, whose mandates cover different aspects and institutions within the Macedonian intelligence sector. However, its ambitious provisions suggest a shift towards enhanced oversight and have the potential to inspire other committees to pursue changes in laws, regulations and practice, in order to improve the parliamentary performance in intelligence oversight. Further steps could be envisaged to develop the legal authority of all three parliamentary committees responsible for the oversight of intelligence sector:

- **Adopt/amend committee rules of procedures.** The enhanced legal authority provided by the Law on Interception of Communications to the relevant committee should be utilized for the development of effective oversight practices, used by the committee routinely. Adopting their own Rules of Procedure (requested by Article 46 of the law) is the necessary next step in developing the legal provisions into practical, detailed guidelines on committee work. The other two committees should follow suit, as intelligence oversight is a joint responsibility.
- **Adopt statutory laws for all intelligence services/departments.** The legislative acts adopted in 2018-19 should only be the beginning of a comprehensive legislative reform of the intelligence sector and its oversight. Similar efforts are underway in many European countries (e.g. France, Germany, the Netherlands, UK). The legal mandate of all agencies and departments who can make use of intrusive methods for information collection should be clearly defined (Intelligence Agency and National Security Agency operate on the basis of a specific law, but this is not the case for the military intelligence service). Ambiguities and overlaps should be avoided in order to create a clear foundation for accountability.

- **Consider adopting special legislation on intelligence oversight.** The inherent challenges in the intelligence oversight process require a strong legal basis and clear procedures for the work of oversight authorities. Instead of having the legal authority for oversight dispersed in several laws and regulations, some countries have opted for adopting a special law to clearly spell out the mandate and powers of oversight bodies (e.g. Germany, Slovenia, Montenegro, Great Britain and Romania). This brings several advantages: it clarifies the rules of the game in oversight and makes the legal authority for oversight incontestable; it contributes to increased visibility, prestige and credibility of oversight authorities; it ensures structural and procedural continuity of parliamentary oversight from one term to the next, contributing to improved institutional memory.

Intelligence oversight is an ambitious, ever changing endeavour. It should be regarded as a continuous work in progress, as despite all the challenges, much work can be done to improve its effectiveness. The main problem in oversight lies primarily in the institutional culture of the intelligence institutions that, granted by the state, have the legal right to use intrusive methods for information collection and other special powers. Enacting legislation is the responsibility of the parliament. But laws can never be formulated so precisely as to exclude all the potentials for abuse of power. The institutions mandated to ensure the rule of law, such as the parliament and the judiciary, must be alert to prevent the exploitation of loopholes.

› WHAT KIND OF LEGAL POWERS DO PARLIAMENTARY COMMITTEES FOR INTELLIGENCE OVERSIGHT HAVE IN THE EU?

Essential powers (20 out of 24 parliaments)

- Oversee services policy and administration, budget and expenditures;
- Receive reports from intelligence services and/or the executive;
- May ask the intelligence services and/or the executive to provide information to the committee.

Enhanced powers (4 out of 24 parliaments)

- Receive complaints from citizens;
- Initiate investigations on their own initiative and inspect premises;
- Issue recommendations or binding decisions;
- Might be involved in the authorisation process of surveillance measures.

Fundamental Rights Agency of the EU (FRA), Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Mapping Member States' legal frameworks, 2015.

2.3.4 Other independent authorities

2.3.4.1 Council for Civilian Supervision

The 2018 Law on Interception of Communications (LIC)[54] established another layer of intelligence oversight, through a civil body mandated to supervise the legality of communications interception. This is an important step towards building public trust in the intelligence sector, especially because a large number of citizens were subject to illegal wiretapping in the past.

54 Law on Interception of Communications, Official Gazette of the Republic of North Macedonia no. 71/2018

The work of the Citizens Supervision Council is closely linked to the Parliament and especially to the Committee for the Oversight of the Interception of Communications. The Council consists of a President and six members (three experts and three representatives of NGOs) appointed by the Parliament from public applications. The Council submits annual report to the Parliament, that is discussed on a plenary session. The premises of the Council must be provided by the Parliament, which allows for closer cooperation and communication between the parliamentary committees and the Council.

Another novelty introduced by LIC is the opportunity for citizens to submit complaints in cases of suspected illegal wiretapping. The Council and the Parliament have shared responsibility in handling those complaints. Namely, the Council receives the complaints and maintains the communication with the affected citizens, but the parliamentary committee is the one responsible for establishing whether an infringement happened or not. Citizens` complaints can be filed in writing at the Parliament archiving department, sent by mail or through filling a specific form. Complaints addressed to the Council must contain a name and surname, date and place of birth of the petitioner, a clear request and the timeline that the compliant refers to[55]. After receiving the complaint, the Council must immediately file an application to the parliamentary committee for the oversight of communications interceptions, requesting them to investigate the complaint. Meanwhile, based on the complaint, the Council performs oversight in OTA and authorized bodies. The committee has 15 days to investigate and report back to the Council (Art. 51.2). For effective joint action in response to complaints, Parliament should develop clear rules and procedures regulating the cooperation and communication between the two bodies.

The powers of the parliamentary committee are more extensive as it can conduct an oversight of OTA, competent authorities and operators by itself or through the technical experts, even without an announcement. Moreover, unlike the Council, the committee can acquire the logs on the time of the launch and completion of the measure for interception of the communications. For the purpose of keeping the confidentiality of the measures for interception of communications, the committee's notification to the Council only informs if the specific case an abuse was identified or not. After receiving the notification, the Council informs the petitioner. In case of abuse, the Council also informs the public (Art. 51/7) and a competent public prosecutor (Art. 51/6).

The Council is also authorized to supervise OTA and the authorised bodies upon its own initiative. In this case, it can conduct oversight only after prior announcement, to access data of anonymized copies[56] of orders from the previous three months; this allows the Council to compare the number of orders for interception of communications, the duration of the interceptions and the identification numbers. The investigatory role of the Council seems therefore to be reliant on the investigative powers of the respective parliamentary committee (see Art. 51/2).

According to the law, the Council adopts its Rules of Procedures regulating issues related to its operations. The Council proceeds with confidential documents in a manner prescribed by law and other regulations in the field, in order to prevent violation of security of classified information and abuse of personal data.

There is a risk of duplication of the work of the Council and the committee (especially in regards with complaints from the public), but also of having diverging views and findings on the work

55 Council Rules of Procedure

56 Anonymization is a process in which all identifying elements listed in the order, including personal and other data, are removed in a way that ensure that the subject of personal data can no longer be directly or indirectly identified.

of the services. The effectiveness of oversight undertaken by these bodies will depend much on the subsequent development of procedures, practices and expertise so that they cooperate and minimize the risk of politicization in oversight.

2.3.4.2 Ombudsperson

The Ombudsperson is an independent, professional institution that contributes to the respect of human rights and fundamental freedoms, and the promotion of democratic values. The ombudsperson is a mechanism for external control of the security sector; it receives and investigates complaints from citizens, including complaints about abuse and misuse of powers or violations of rights committed by security sector personnel. The mandates of the ombudsperson institutions vary significantly across Europe but most do not play a significant role in intelligence oversight. Even when laws allow them specifically to investigate citizens' complaints about security and intelligence services they rarely do so in practice. Their impact on the conduct of services or in situations when human rights have been infringed is limited, because most often they only issue recommendations.

The role played by the Macedonian Ombudsperson in the intelligence oversight could be significant, given the mandate it was given by national legislation. The legal basis for the work of the office of ombudsperson derives from Article 77 of the Macedonian Constitution, which empowers it to "protect the constitutional and legal rights of the citizens when violated by bodies of the state administration and by other bodies and organisations having public mandates." Every citizen has the right to submit a complaint to the Ombudsperson - who is elected by the parliament for a term of eight years, renewable once.

The Law on Ombudsperson adopted in 2003[57] grants it a clear mandate and strong investigative powers which are in line with the Paris Principles and other applicable international documents. The Ombudsperson can initiate investigations on his/her own authority (Art.13) given probable cause, or the possibility that abuses may be taking place. It has the authority to compel public institutions to provide information and detailed explanations regarding any complaint in a timely manner; it is also entitled to enter institutions` premises and inspect their documentation (Art.24). All state officials (including the heads of intelligence services) must comply, whether or not the information requested is classified (Art. 27). Once the Ombudsperson determines that there has been a violation, he/she is entitled to: suggest ways in which to remove the obstacle(s) found, initiate disciplinary proceedings or request that the Public Prosecutor initiate a criminal investigation (Art.32).

The new Law on Interception of Communications (Art. 56) assigns the Ombudsperson with a specific role in the supervision over the legality of interceptions, from the aspect of protection of human rights and freedoms.

However, despite this strong legal authority for oversight, the Ombudsperson has not been an active human rights defender between citizens and the security and intelligence sector. The Ombudsperson especially focuses on developments related to observance and protection of constitutional and legal rights of persons in institutions and organizations where freedom of movement is restricted.

When the Ombudsperson establishes that the constitutional and legal rights of the petitioner have been violated or other irregularities have taken place, it can:

57 Law on the Ombudsperson, Official Gazette of the Republic of Macedonia no. 60/2003, 181/2016, 189/2016, 35/2018 and Decision of the Constitutional Court of Republic of Macedonia, Official Gazette of the Republic of Macedonia no. 111/2007

- provide recommendations, proposals, opinions and indications on the manner of removing such violations;
- propose a re-administering of a certain procedure in compliance with the law;
- launch an initiative for disciplinary proceedings against an official or file a request to a competent public prosecutor to initiate proceedings for the purpose of establishing penal responsibility.

The Ombudsperson submits a publicly available annual activity report to the Parliament and presents it during a plenary session attended by representatives of the Government. This could be an opportunity for the Parliament to engage in more detailed dialogues with the Ombudsperson, trying to exchange lessons learned and develop complementarity of action.

2.3.4.3 Agency for Personal Data Protection (APDP)

Respect and protection of people's privacy, as well as security and secrecy of personal data, are freedoms and rights guaranteed by the Constitution of the Republic of North Macedonia. Their actual safeguarding began with the establishment of the Directorate for Personal Data Protection in 2005, renamed into Agency for Personal Data Protection through adoption of the Law on Personal Data Protection in 2020[58].

APDP is an independent state authority managed by a director elected and dismissed by the Parliament, for a 5-year term. It submits an annual report to the Parliament, as well as additional reports if requested.

APDP is one of the most important independent supervisory authorities when it comes to intelligence oversight, considering that the services collect and process large amounts of sensitive personal data. It is also one of the competent authorities for the oversight of measures for interception of communications, establishing the legality of undertaken activities when processing personal data and the measures taken for their protection. The legal responsibilities intelligence services have in the field of personal data protection mainly refer to:

- The legality and legitimacy of processing personal data in intelligence work.
- The implementation of relevant technical and organizational measures that minimize the risk of possible abuse.
- Ensuring that, in cases where abuses occur they leave a trace that no one can alter, thus enabling a swift reaction, and a clear division of duties and responsibilities of those who are processing personal data within the security-intelligence services

APDP ensures a systemic and independent control of the legality of processing personal data, including research, inspection, giving guidelines and providing training on personal data protection. Regular supervision is carried out in line with the annual programme, but extraordinary supervision can be also conducted at the proposal/initiative of a state authority a legal entity or natural person, ex officio or if the supervisor suspects of a violation of the Law on Personal Data Protection. Moreover, a supervisory control can also be carried out in order to remove the established violations.

When conducting an inspection, the Agency`s supervisor[59] has the right to:

- check for general and individual files, documents, computer files, information and other evidence, in a volume according to the subject of the supervision, ask and keep copies in hardcopy or electronic form;
- control business or official premises and other facilities that carry out personal data

58 Law on Personal Data Protection, Official Gazette of the Republic of North Macedonia no. 42/2020

59 Art. 105, Law on Personal Data Protection, Official Gazette of the Republic of North Macedonia no. 42/2020

processing, or seek insight into their processing;

- conduct insight into personal identification documents for confirming their identity in compliance with the law;
- ask the controller, i.e. processor for written or oral explanation of affairs within the scope of the supervision;
- ask for expert analysis and opinion when necessary for the supervision;
- use technical means to take photos and videos that can be used in the supervision;
- assess the equipment used for personal data processing and the equipment where personal data is kept, check the IT system and IT infrastructure in which the personal data processing is being conducted, accompanied by a representative of the controller, i.e. the processor;
- use communication devices of the controller, i.e. the processor for the purpose of meeting the goals of the supervision; and
- secure other required evidence in accordance with the subject of the supervision.

A report is issued upon each supervision, indicating the findings and possible violations of personal data protection provisions. If the recommendations issued are not addressed by the institution, APDP notifies Government or Parliament with special report. APDP also submits an annual report to the parliament, published on the webpage of the Agency[60]. APDP reports are a useful tool for oversight into the work of security and intelligence services with regards to personal data processing: the implementation of recommendations made in these reports can be followed by parliament, who can ask information and explanation about measures and actions taken in order to correct irregularities identified during the Agency supervision.

› WHAT ARE THE INTERNATIONAL GOOD PRACTICES ON INTELLIGENCE COLLECTION, MANAGEMENT AND USE OF PERSONAL DATA?

Practice 21. National law outlines the types of collection measures available to intelligence services; the permissible objectives of intelligence collection; the categories of persons and activities which may be subject to intelligence collection; the threshold of suspicion required to justify the use of collection measures; the limitations on the duration for which collection measures may be used; and the procedures for authorizing, overseeing and reviewing the use of intelligence collection measures.

Practice 23. Publicly available law outlines the types of personal data that intelligence services may hold, and which criteria apply to the use, retention, deletion and disclosure of these data. Intelligence services are permitted to retain personal data that are strictly necessary for the purposes of fulfilling their mandate.

Practice 24. Intelligence services conduct regular assessments of the relevance and accuracy of the personal data that they hold. They are legally required to delete or update any information that is assessed to be inaccurate or no longer relevant to their mandate, the work of oversight institutions or possible legal proceedings.

Practice 25. An independent institution exists to oversee the use of personal data by intelligence services. This institution has access to all files held by the intelligence services and has the power to order the disclosure of information to individuals concerned, as well as the destruction of files or personal information contained therein.

UN, Human Rights Council, Martin Scheinin (2010)

60 Art. 67 and 70, Law on Personal Data Protection, Official Gazette of the Republic of North Macedonia no. 42/2020

A systemic control over personal data protection by intelligence services should follow the application of the following **principles**:

Legality - personal data should be processed in line with the law, sufficiently and transparently in relation to the subject of personal data, taking into consideration the specifics of intelligence, where transparency is often (justifiably) limited ("legality, fairness and transparency");

Legitimacy - personal data should be collected for specific, clear and legitimate purposes;

Proportionality - personal data which is processed should be appropriate, relevant and restricted to what is necessary regarding the objectives it is processed for ("minimum data volume");

Accuracy - personal data should be accurate and stored in a form that ensures identification of personal data subjects, and not longer than necessary for the purposes that personal data is processed for; and

Physical protection - personal data should be processed in a way that ensures a proper level of security, including protection from unauthorized or unlawful processing, as well as their accidental loss, destruction or damaging, by using relevant technical or organizational measures.

Given that the weakest link in IT safety is the human factor, one of the most important things oversight needs to ensure is that the **proper technical and organizational measures** are applied when processing personal data.

› QUESTIONS THAT COULD GUIDE AN ASSESSMENT OF TECHNICAL AND ORGANIZATIONAL MEASURES UNDERTAKEN FOR DATA PROTECTION:

- Have risk of processing personal data identified, assessed and classified (risk analysis)?
- Is technical and integrated personal data protection applied?
- Is there any record of activities (operations) for personal data processing?
- Is staff aware on privacy and security risks and trained on personal data protection?
- How is security of personal data processing ensured ?(pseudonymization and encrypting of personal data; ensuring continual confidentiality, integrity, accessibility and resilience of processing systems; capability for timely reestablishment of availability of personal data and access in case of physical or technical incident; regular testing, assessment and evaluation of the effectiveness of technical and organizational measures in order to guarantee the security of the processing)
- What is the manner of ensuring the authentication of authorized persons in the IT system?
- What is the manner of ensuring the control of access to IT system?
- What is the manner of ensuring the registration of every access in the IT system?
- What is the manner of managing incidents? (incidents that violate confidentiality, integrity or availability of personal data)
- What equipment is utilized when personal data is processed?
- How is the internal network of the intelligence services protected?

- How are servers and websites secured?
- How is processed personal data that has been pseudonymized or encrypted?
- What are the tasks and responsibilities of the IT system administrator and the authorized persons when using documents and ICT equipment?
- What procedures are there for reporting, reaction and incident recovery?
- What procedures are there for crating safe copies, archiving, storage, and recovery of stored personal data?
- How are documents destroyed, and what procedures are there for destroying, deleting and cleaning electronic storage media?
- Is there an effective system in place for registration of authorized access (logs), which incorporates use of measures and controls that ensure an information security audit trace through registration of authorized access (logs) in IT systems where personal data is processed, including: name and surname of authorized person, work station for access to IT system, date and time of access, personal data that has been accessed, type of access and undertaken operations when processing data, authorization log for each access, log on each unauthorized access and log on automated rebuttal from the IT system. The records should also incorporate the input of identification data of the IT system wherefrom an external attempt is made to access the operational functions or personal data without having the required authorization level (log management that provides "input", "edit", "update", "delete" and "view log);
- Is transfer of information that contains personal data carried out by using special protection and relevant methods guaranteeing that data will not be legible during the transfer (encrypted or in another relevant format)?
- Is physical access to servers, hardware, electronic storage media where personal data processing is carried out, provided only to authorized persons (physical security of equipment in intelligence services)?

2.3.4.4 Directorate for Security of Classified Information

The Directorate for Security of Classified Information[61] is an independent state authority mandated to implement the policy of classified information protection. It is managed by a director appointed and dismissed by the Government, for a 4-year term. The Directorate is divided in three sectors: (1) Sector for General and Legal Affairs and Support to the Director, International Cooperation and Inspection Oversight,

(1) Sector for General and Legal Affairs and Support to the Director, International Cooperation and Inspection Oversight,

(2) Sector for Administrative, Personnel and Industrial Security of Classified Information, and

(3) Sector for IT and Physical Security.

The Directorate for Security of Classified Information controls and oversees the compliance with procedures for handling classified information in state authorities, judicial authorities, local self-government units, trading associations, public enterprises, institutions and services of significance for protection, use and international exchange of classified information, other legal entities and natural persons. According to the Law on Interception of Communications,

61 Law on Classified Information, Official Gazette of the Republic of North Macedonia no. 275/2019

the Directorate is the oversight authority with the task of establishing the legality in proceeding with classified information of OTA and competent authorities.

Oversight inspections are carried out by inspectors for security of classified information, who are authorized to review the implementation of law and regulations in the field and to propose measures for removing identified irregularities and shortcomings within a specified deadline. Inspections can be regular, extraordinary and controlling.

- Regular inspections are carried out in line with the annual programme,
- Extraordinary inspections are conducted on the basis of an initiative by relevant stakeholders or ex officio (inspector's suspicion).
- Control inspection are carried out after the expiration of the deadline for removal of identified shortcomings.

During inspections, inspectors have the right to access at any time and without announcement facilities, business premises, residential buildings or offices in which classified information is handled or stored.

A misdemeanour procedure is initiated if the inspector establishes a violation of a law or regulations, or other wrongdoings. If the inspector establishes the existence of a crime, the director is immediately notified for the purpose of initiating a procedure before a competent authority.

2.3.4.5 State Audit Office (SAO)

The most important institution when it comes to ensuring the financial accountability of intelligence services is the State Audit Office (SAO). This independent state institution consists of professionals specialized in detecting financial irregularities.

Relations between Parliament and SAO are regulated by the Law on State Audit. The head and deputy head of the SAO are elected by the Parliament for a period of 9 years. The yearly program of the SAO is submitted to Parliament solely for information.[62] The SAO also submits individual reports on completed audits and the yearly report for its work, but only the yearly report is subject to debate in Parliament. Individual reports on completed audits of the intelligence services have not yet been discussed with the relevant committees[63].

The Sector for audit of entities in the legislative, executive, state administration authorities and public enterprises, defence, public security, judiciary, public prosecutor's office and state attorney's office is responsible for oversight of intelligence services. This sector has a department for budget audit, including stakeholders in the fields of defence and public security.

In the performance of its mandate, SAO has access to classified information. This includes free access to the official premises and the property of the audit subject, right to have insight in the books, forms and other documents, electronic data and IT systems, as well as the right to ask for explanations on all issues of significance for the audit. When performing an audit for specific areas, the State Audit Office can hire professionals and experts in the field. Since the access to intelligence services documentation is limited for other oversight institutions, SAO could play a key role in intelligence accountability. Therefore, it is important that the SAO pays attention to the financial reports of the intelligence services and conducts regular audits on their expenditures. Strengthened communication between oversight committees and SAO

62 Art. 23 , Law on State Audit, Official Gazette of the Republic of Macedonia no. 66/2010, 145/2010, 12/2014, 43/2014, 154/2015, 192/2015, 27/2016 and 83/2018

63 SAO conducted an audit in the Intelligence Agency in 2007

(through a better exchange of information and even through planning joint action) could contribute significantly to enhancing the financial accountability of intelligence services and departments.

2.3.4.6 State Administrative Inspectorate

The State Administrative Inspectorate[64] is an authority within the Ministry of Information Society and Administration, with legal entity capacity. Its objective is to conduct oversight over the implementation of the Law on General Administrative Procedure, Law on Oversight Inspection and other laws containing provisions on administrative procedure. The State Administrative Inspectorate is divided into a Sector for Oversight Inspection-East and Sector for Oversight Inspection-West.

The oversight conducted by the State Administrative Inspectorate relates to:

- timely, economical and efficient realization of the rights and interests of citizens and other stakeholders in the administrative procedure when resolving administrative affairs;
- proceeding within the prescribed deadlines in first-instance and second-instance administrative procedure, as well as within deadlines given in acts of judicial authorities;
- enforcement of administrative acts;
- receiving complaints;
- conduct and operations by administrative officers and employees for the purpose of ensuring observance of the principles of legality, professional integrity, efficiency, responsibility and loyalty when executing their duties etc.

When conducting oversight, inspectors are authorized to get direct insight into the implementation and enforcement of regulations related to office operations, inform the overseen institution about identified shortcomings and irregularities in operations, and order the correction of identified shortcomings within a prescribed deadline. The inspector compiles a summary of the oversight inspection, including a finding on the current situation, whereas the identified shortcomings can be removed through a decision that provides the deadlines for their enforcement. The oversight inspection can be regular, extraordinary and controlling.

The significance of the State Administrative Inspectorate in conducting intelligence oversight is based on identifying the irregularities in administrative operations, protection of citizens' rights and protection of the public interest.

2.3.4.7 Agency for Protection of the Right to Free Access to Public Information

The Agency for Protection of the Right to Free Access to Public Information[65] is an independent state authority mandated to ensure the transparency of public institutions and the respect of the right to free access to public information, for natural persons and legal entities.

The significance of this Agency in the oversight of intelligence services arises from its power to conduct administrative procedure and decide on complaints against a decision by which the information holder had rejected the petitioner's request for access to information.

64 Law on Administrative Inspection, Official Gazette of the Republic of Macedonia no. 69/2004, 22/2007, 115/2007, 51/2011, 164/2013, 41/2014, 33/2015, 156/2015, 193/2015, 53/2016 and 11/2018

65 Law on Free Access to Public Information, Official Gazette of the Republic of North Macedonia no. 101/2019

2.3.4.8 Public Internal Financial Control Department

Public internal financial control is an integral element of the national public finance management. It represents a comprehensive concept that relates to the entire public sector, especially the revenues and expenditures of the central authorities, including foreign funds. It aims to ensure that

- public funds are spent in the right, ethical, economical, effective and efficient way;
- operations are following laws, regulations, established policies, plans and procedures;
- property and other resources are protected from losses caused by poor management, unjustified spending and use, irregularities and abuse.

The Public Internal Financial Control Department[66] is part of the Ministry of Finance and it aims to coordinate the development, establishment, implementation and maintenance of the system of public internal financial control, which incorporates financial management and control, internal audit and their harmonization.

Intelligence services must use the funds allocated from the state budget in a transparent, economical, efficient and effective way. Financial management and control must be implemented at all levels within the services, in respect with the spending of the budget allocation, but also in the spending of funds provided by the European Union, other donors and extrabudgetary sources.

2.3.5 Public prosecutor/Judiciary

Judicial control is one of the most powerful safeguards in the use of intrusive methods, therefore legislation should clearly prescribe applicable principles for ex-ante judicial approval of a measure and for ex-post judicial review, during the implementation and upon termination of the measure. These principles (such as legitimacy, proportionality, legality, necessity, subsidiarity or ultima ratio) should be binding for all state authorities involved in the initiation, authorisation and implementation of intrusive methods for information collection.

Besides the authorisation of these measures, the judiciary undertakes several other actions of relevance for intelligence oversight:

- *Adjudicates charges of misconduct*, criminal activity or access to information in issues related to intelligence. So that secrecy does not lead to impunity, special judicial provisions can ensure that the law is applied even while protecting classified information;
- *Provides access to a legal remedy* in cases when individuals complain about infringements of their rights or discrimination by security and intelligence services, files a complaint and challenge an arrest, interrogation, detention or an interference with their privacy;
- *Conducts judicial review* that ensures all intelligence-related laws and policies created by the legislature or the executive are compatible with the constitution;
- *In many countries, assists* parliamentary or independent oversight, judicial officials (or retired members of the judiciary), in contributing their expertise to parliamentary enquiries or oversight commissions on conducting special inquiries.

Judicial protection as a general principle in the use of intrusive measures has been somewhat neglected in the past (not only in North Macedonia but also in most countries), for even when judicial authorization for surveillance was sought and obtained, this was in practice a mere

66 Law on Public Internal Financial Control (Official Gazette of Republic of Macedonia no. 90/2009 and 188/2013)

formality. The judges did not have, or did not regard themselves as having, a responsibility to check if the surveillance was justified on material grounds. Instead, judges only checked the formalities (e.g. if the offence for which surveillance is being sought is one that allows for surveillance). Today, such a restricted approach to judicial authorisation goes against European standards, and the state of play is also improving in the Republic of North Macedonia. A failure of the judiciary in controlling the use of special powers by intelligence services is considered to be a failure for democracy and the rule of law.

The constitutional setup and powers of the public prosecutor's office arise from its relationship with other authorities that are actively involved in crime detection and prevention. The public prosecutor's office is concerned about the legality of measures and actions undertaken in the pre-investigative procedure and safeguards the observance of law and human rights by members of intelligence services. The control of the public prosecutor as a state authority provides them with the right to realize an expert oversight and insight into the operations of intelligence services. Moreover, the controlling activity is also realized through assessment of the criminal charge that is forwarded to the public prosecutor, who can establish that the evidence contained there have not been collected in a legitimate way.

The judiciary plays an important role in the proposition, approval and implementation of special investigative measures in the Republic of North Macedonia. Its role is evident in regard to interception of communications, as described in the Law on Interception of Communications.

The law ensures two levels of control in the implementation of the interceptions of communications for purposes of both criminal investigations and national security and defence[67], with the Public Prosecutor and the judge issuing the order for interception of communications[68] . Their control covers the legality of the implementation of the measures and the subjects of control are the competent authorities, the telecom operators and the OTA. Besides authorising the measures, the legislators also provided strong powers to the judiciary: unannounced inspections of sites, equipment and documentation, direct access to the electronic registry system, control over the use of special technical devices and equipment etc.

The State Public Prosecutor of the Republic of North Macedonia submits an annual report to the Parliament that must contain information on the implementation of special investigative measures. The committee overseeing interception of communications shall consider this report as part of their task to conduct oversight of the efficiency of interception of communications.

As in most European countries, the main system of control over surveillance in the Republic of North Macedonia is the judiciary, relying on prosecutors and the courts. The oversight provided by parliamentary committees and citizens council are intended as "back-up". If the prosecutors do not act as a filter on surveillance applications, and the courts do not take authorisation and supervision mandates seriously, then the "back-up" systems will not be able to compensate for this failure of control. At best, what they can do is to reveal a failure in judicial control.

67 In many European countries, the applications for use of intrusive methods for information collection by intelligence services for purposes of national security are delivered directly to the competent judge, without the prosecutorial filter.

68 The pre-investigative judge issuing the order for a special investigative measure based on the law and the Supreme Court judge issuing the order for interception of communications respectively, Law on Interception of Communications, Articles 57-61.

› WHAT IS THE DIFFERENCE BETWEEN PARLIAMENTARY OVERSIGHT AND JUDICIAL OVERSIGHT?

- Parliamentary oversight focuses more on policies, while judicial oversight deals exclusively with narrow legal issues; the judiciary only reacts to legal matters brough to its judgment, it cannot take initiatives on its own;
- Parliamentary oversight is, in theory, unlimited. MPs have the democratic legitimacy to ask for information and explanation on any aspect of the work of a government agency, and have the right to inspect premises and check intrusive capacities themselves;
- Judges tend to demonstrate more deference to the executive branch on issues of national security and intelligence compared to MPs;
- Although parliaments usually have little authority on operational affairs, they have extensive powers to determine the mandate and budget of security services, which gives them important leverage in influencing their conduct.

3

COMMITTEE OVERSIGHT ABILITY: ENABLING CONDITIONS FOR EFFECTIVE OVERSIGHT

For oversight to be credible it needs to rely on a clearly defined **legal authority**, be embedded in Constitution and laws, and meet the democratic standards that make checks and balances functional and accountability a fundamental principle of governance. The previous chapter of this Guideline reviewed the legislative framework that gives the parliament legal authority to engage in intelligence oversight. Institutions and legal provisions making intelligence oversight possible are in place. 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. This chapter will review the conditions that enable committees to make full use of their legal authority and engage in effective intelligence oversight.

Parliamentary oversight is a function of the whole parliament, but it is more efficiently and visibly developed at committee level. A well institutionalized structure of standing committees[69], 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. They pursue the accountability of executive agencies (including intelligence services), from two main points of view:

1. 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;
2. political - evaluating the political choices of the executive, their consistency with national interests and the program of the government, their implementation and consequences.

WHAT ARE THE LEVELS OF ACTION IN PARLIAMENTARY OVERSIGHT?	
PLENARY SESSION	**Endorsement of security policy/strategy and of government's policy** **Enactment of laws** **Approval of the use of public funds (State Budget Law)** **Motions and votes of confidence** **Consent to top appointments (ministers, intelligence directors)**

69 Ad-hoc committees may be appointed with a specific mandate, such as a particular bill or an issue under investigation, that dissolve after finishing their mandate.

COMMITTEES	**Legislative reports, oversight reports** **Recommendations** **Hearings and inquiries** **Visits and inspections on the field** **Investigation of citizens' complaints**
MEMBERS OF PARLIAMENT	**Legislative initiatives and amendments** **Political declarations** **Questions and interpellations (in the plenary, oral or written)** **Requests for information (free or classified)**

3.1 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, while 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 modalities 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 of the committee – it should describe the issues and/or institutions 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 modalities for engaging with overseen institutions.
- The rights and responsibilities of the chairperson, deputies and staff.
- The procedure of calling and running a committee meeting, including the size of quorum (important for avoiding blockages from the chairperson if he/she is the only one left in charge).
- The rules of debate and vote – must ensure that minority groups can express their views and participate in the decision-making processes.
- The possibility of having a member represented by other colleagues in case of unavoidable absence.

HOW DO PARLIAMENTARY OVERSIGHT COMMITTEES ORGANISE THEIR WORK?

- Adopting committee Rules of Procedure.
- Clarifying their mandate and priorities: legislation or oversight; policy, budgets or operations?
- Deciding on the profile of the administrative and expert staff they need; convince the parliament (the Budget Council, Art.27 of Law on the Assembly) to allocate sufficient funds to the committee to afford employing the needed experts (both for permanent and temporary/specific support).
- Establishing 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 the respective issues and regularly inform the committee on its evolution, plan and organise concrete oversight activities in that area, ensure regular communication with the overseen service on that issues, identify committee needs for external expertise on that matter.
- Identifying independent sources of information and expertise, outside the intelligence and executive: academia, national and international think tanks, civil society organisations etc.
- Considering what tools of oversight to use in order to gain a good understanding of intelligence structures and processes – request briefings, following up reports from the agencies, organising field visits and inspections, calling intelligence personnel to hearings, addressing questions and interpellations in the plenary etc. Plan for the utilization of specific oversight tools according to specific oversight objectives and priorities.
- Deciding on an Annual Activity Plan, to facilitate planning, engagement of expertise, and communication with intelligence services (see Annex 3).
- Establishing 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.

3.2 JOINT MEETINGS AND OVERSIGHT ACTIVITIES

The Macedonian parliament has put in place a complex and specialized institutional mechanism for intelligence oversight, composed of three parliamentary committees and one Council for Civilian Supervision. The composition, tasks, workload, transparency and objectives of these bodies varies. There are overlaps between their mandates, but there might also be aspects of intelligence work that slip between, enabling the services to avoid meaningful oversight if that is what they want. Communication, expert collaboration and joint action between committees are indispensable for several reasons.

1. **Understanding intelligence better.** The intelligence sector is big and 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.

2. **Pooling resources and expertise.** The resources (staff, time, budgets) for oversight are always very small compared to the resources of those being overseen; therefore, it is vital that they are leveraged in order to have more impact. The expertise developed by each committee in their area of expertise and their experience in engaging in effective oversight needs to be shared with the others. This is a small step towards rectifying the information asymmetry among the intelligence services and the parliament.

3. **Creating increased political leverage.** By working together, committees can better influence the executive and the intelligence sector. Committees have no power of enforcement; their recommendations are not legally binding for 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 recommendations. When acting together, committees have increased legitimacy and their united voice has considerable political importance.

For these reasons, developing cooperation and complementarity of action between security 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 organise joint hearings of public officials or joint study visits/inspections in the field.
- Formally, it 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, so the current RoPs should be amended accordingly, 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 three 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 cooperation and the exchange of information and expertise with the Council for Civilian Supervision (see section 3.2.4.1.) will have to be considered carefully, especially by the committee for the oversight of interceptions.

The key principle in organising 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.

3.3 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 function of Macedonian 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.

1. **Democratic oversight expertise** – a good understanding of the importance of oversight and the function of the 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, or 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.

2. **Legal expertise** – a clear understanding of the strategic framework and all relevant law and regulations underpinning intelligence activity in the Macedonian state. 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 overridden for national security reasons;

- the use of special powers such as the recruitment of agents or interception of communications;
- data protection, including any relevant EU laws and directives;
- Citizens' and service employees' complaints, including what protections exist for intelligence staff, such as protection from illegal order or whistle-blower protection.

3. **Operational expertise** – an understanding of how services really function. Whether committee members have prior experience of 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.
4. **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.

› EXPERTISE AVAILABLE TO OVERSIGHT BODIES IN THE 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 it 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. The IPCO is more engaged in the oversight rather than review part of the system, with the responsibility to oversee 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 of:

- **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 when specific requirements demand.

In this way, the IPCO provides day-to-day oversight of intelligence activities, as well as 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 years (minimum 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, the 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.

The important work of the parliamentary staff rarely gets the credit it deserves. **Committee staff** prepares and organises committee meetings, maintains contacts with government agencies, collects information and helps interpret government information. They must cover a wide range of activities, from secretarial work to juridical advice, drafting legislation, planning and organising oversight activities, drafting reports, research papers or speeches. Staff supporting security and intelligence committees should have access to classified information, in order to complete their job. Stable professional staff is essential to make committees able to meet their responsibilities; they ensure the continuity of expertise and the institutional memory of a committee.

The provisions of the new Law on Interception of Communications (Art.39) show a strong recognition of the need to boost expertise in the oversight of complex technical issues such as interceptions[70]. The implementation of these legislative provisions will better equip the responsible committee to engage in an informed dialogue with the overseen institutions and undertake more efficient examinations and investigations. Two practical questions will need to be resolved with the implementation of the law:

- How will the budgetary implications of the law be addressed? How will the parliament fund the employment of the supplementary expertise (two permanent support staff, roster of experts employed case by case, staff seconded by other state institutions) provided by the law?
- How will the other two committees (defence and security; intelligence oversight) and the Citizens Supervision Council recruit and develop the expert support they need? The law does not make any reference to the administrative and expert support needed for the functioning of the Council. Will they be able to draw on specific technical expertise employed by the interception oversight committee when needed?

70 Art. 58 of the Law also refers to hiring experts - to support the relevant judicial bodies that control the implementation of interceptions.

› SOURCES OF ENHANCED COMMITTEE OVERSIGHT ABILITY

- Access to information
- Clear and detailed committee procedures
- Parliamentary staff: use of 4 circles of inner expertise
  1. Personal advisors
  2. Parliamentary group staff
  3. Committee staff
  4. Specialised departments (such as the Parliamentary Centre, legislative department)
- The use of external expertise: academia, NGOs,
- Cooperation with other oversight bodies: National Audit Office, Ombudsman, Civil Supervision Council, Data Protection Agency

3.4 ACCESS TO INFORMATION

Most European parliaments have privileged access to classified information in order to oversee intelligence services. The parliament's right to be informed by the executive is the first condition for effective law-making and oversight.

In security and intelligence matters, the access to information raises challenges related 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 to the parliament and the public. However, a distinction must be made between "the need for confidentiality", which is understandable and manageable, and its extreme interpretation, "lack of public scrutiny", which is unacceptable in a democracy.

› ACCESS TO CLASSIFIED INFORMATION BY OVERSIGHT BODIES IS A WIDELY ACCEPTED INTERNATIONAL STANDARD.

"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 fulfil 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."[71]

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.

71 UN Human Rights Council, Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight A/HRC/14/46 (2011), Practice 7, see: https://fas.org/irp/eprint/unhrc.pdf

(1) 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[72]. 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. This access to classified information does not mean that MPs are exempt from legal sanctions for unauthorised disclosure of secret information.

(2) In other parliaments, committee members obtain access to classified information only after receiving a security clearance (some examples are Estonia, Hungary, Latvia, Lithuania, Poland, Serbia and Macedonia). The security clearance is issued after MPs undergo background checks performed by a governmental agency (usually the domestic intelligence service or the police). The checks provide a risk assessment and they refer 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 mechanisms. 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. It clarifies the rules of the game and empowers MPs in their dialogue with executive officials.

However, 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. 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.
- Granting a person a security clearance does not mean they will not make 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 unauthorised disclosure. However, consistent dialogue between parliament and the services builds up the necessary awareness and responsibility. In most states, parliamentarians do not normally enjoy immunity from prosecution in the case of an unauthorised disclosure of information.

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

72 See for example the case of Netherlands: http://www.ennir.be/netherlands/intelligence-review-netherlands

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, 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 to the access to 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 the discretion) to define the *need to know* of a parliamentary committee falls completely on the executive. Then, the parliament's access to information depends on how ministerial discretion, and the parliament has limited or no way of challenging such decisions.

› HOW IS COMMITTEE ACCESS TO INFORMATION REGULATED IN SOME COUNTRIES?

- **Germany** – the Parliamentary Oversight Panel has the right to request information, documents and other files including data from the federal government and the three intelligence services. Demands must be met immediately. The staff of intelligence services can also be questioned; members of the Oversight Panel are sworn to secrecy, they can publicly comment on certain issues as long as the decision to do so is reached by two-thirds of the members. The Oversight Panel may request expert witnesses to provide evaluations. (Parliamentary Control Panel Act)
- **Romania** – the Intelligence Oversight Committee (for the domestic intelligence service SRI) can request reports, briefs, press releases, explanations, documents, data and information; they can summon military and civilian personnel of the service to hearings. SRI is obliged to provide the required information to the Committee within 7 working days. If this deadline is not met, SRI is obliged to explain the reasons and notify on the time needed for the preparation of the requested information. (Parliament decision no.85/2017)
- **Hungary** – two thirds of the National Security Committee can vote to require the executive/the service to disclose specific information regarding the operating methods of the intelligence service. (Act CXXV/1995)

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:

1. 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 (for example patterns of targeting and targeting priorities).

2. **Information relating to sources and methods** used [73]. Identities and roles of human sources are among the most sensitive aspects of intelligence work. Leaks of sources' identity can jeopardize their personal safety whereas dissemination of information about methods could render methods ineffective, give advantage to adversaries and endanger 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.

3. **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"[74]: information provided by a foreign entity cannot be transmitted to a third party or used for any other purpose that was not agreed upon, without the prior consent of 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.

4. 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.

› WHAT KIND OF INFORMATION IS EXEMPT FROM ACCESS IN DIFFERENT NATIONAL LAWS?

- Ongoing or future intelligence operations, information that could disclose the identity of undercover agents, sources, methods or tools. The exception from access does not apply in situations where a court establishes violations of human rights and freedoms (Romania)
- Documents of foreign services or documents that could affect the personal rights of third parties (Germany)
- Information that could endanger the national interests or safety of persons (Austria)
- Information that could endanger the security of the Republic (Italy)
- Sensitive information (UK)
- Operationally sensitive information (France)
- Information that could disclose the identity of a source or impair the rights of third parties (Luxembourg)

73 This is not related to the services' operating methods that are public and known in general, but the specific methods applied in a relevant case, which exposure would result in big damages to the case, the service's work and a possible endangerment of human lives.

74 Sometimes referred to as 'originator control' (ORCON)

3.4.1 Parliament handling of classified information

Efficiency cannot be expected from parliamentary oversight committees in the field of defense, security and intelligence if there is no access to relevant classified information. But legal access to classified information should not result in unauthorised disclosures, which could create risks for national security and compromise intelligence and security operations. There are different safeguards designed to prevent such security incidents:

- Access to classified information is permitted based on the **"need to know"** principle. Parliamentarians can have access to information only if this is necessary in the execution of a specific oversight mandate.
- MPs get a security certificate after going through a **security vetting** process which involves a background check of their reliability and trustworthiness. Appeal mechanisms must be envisaged by law, in cases a security certificate is denied; for these to be effective the agency who does the backup checks should be obliged to explain why clearance was not granted.
- MPs are required to sign **an agreement of non-disclosure** of information, or take a secrecy oath, at the beginning of their tenure in security and intelligence committees.
- Unauthorized disclosure of classified information can lead to administrative and/or penal **sanctions** according to the law, MPs making no exception. In most states, parliamentarians do not enjoy immunity from prosecution in the case of an unauthorised disclosure of classified information.
- **Staff** supporting the activity of security and intelligence committees is vetted and gets a security clearance.
- **Officers for the security of classified information** are appointed in Parliament[75] (as in other state institutions that are handling classified information), to ensure an efficient and coordinated execution of the rights and obligations related to access to classified information and handling of classified documents. They are responsible for the implementation of the Law on classified information and international agreements related to the security of the classified information in the institution[76]. They also inform, guide and ensure appropriate trainings for MPs and staff on all necessary measures for the protection of classified information and the personal protection of the users.

The main condition for the functioning of these arrangements is the professional conduct of members of parliament and the committee support staff.

75 Art. 65 of the Law on classified information, Official Gazette of the Republic of North Macedonia, no. 275/2019

76 Art. 68 of the Law on classified information, Official Gazette of the Republic of North Macedonia, no. 275/2019

SECURITY VETTING IN THE MACEDONIAN PARLIAMENT

All elected members of the Macedonian Parliament may apply for the issuance of a security certificate. This applies to the members of the three committees holding competency over defence and security, intelligence, and communications interception oversight; they are not required to apply for and to get a security clearance, but they do need a security certificate if they want to participate to committee meetings or activities where classified information is discussed and/or handled.

The bacground checks are conducated by NSA. Based on the NSA opinion, the Directorate for Security of Classified Information takes the decision wheather to give a securtiy clearance or to reject the request. If the securtiy clearance is denied, the Directorate has no legal obligation to elaborate the reasons. The law provides however for an appeal mechnisms in case of a negative decison[77] .

The Committee for the oversight of NSA and IA have the legal power to investigate how background checks are conducted and may get insights in the facts and evidence that determined such a negative decision. The oversight investigation of security checks procedures may:

- counterbalance the monopoly of information exercised in the security check,
- prevent possible subjectivism, discretion and abuse
- contribute to overall accountability of intelligence services.

The Macedonian Law on Classified Information[78] provides the legal framework for the classification of information, conditions, criteria and measures undertaken for its protection and security, the rights and responsibilities of classified information creators and users, as well as national and international exchange of classified material. This law is adapted to European regulations[79] and guarantees a high level of harmonization with NATO standards for handling classified information. The objective of the law is to ensure legitimate use of classified information and eliminate any kind of illegitimate or unauthorized access, abuse and exposure of information. The obligation to protect classified information belongs to all beneficiaries of classified information who had access and/or were acquainted with its content. The levels of classification and their protection are proportional to the degree of damages incurred by unauthorized access or unauthorized use of the information to the national interests.

77 Articles 57 and 58 of the Law on Classified Information, Official Gazette of the Republic of North Macedonia, no. 275/2019

78 Law on Classified Information, Official Gazette of the Republic of North Macedonia no. 275/2019

79 This law makes an alignment with the Council Decision of 23 September 2013 on the security rules for protecting EU classified information, CELEX no 32013D0488

LEVELS OF INFORMATION CLASSIFICATION IN THE REPUBLIC OF NORTH MACEDONIA [80]

- Classified information level **"TOP SECRET"** is information, unauthorized disclosure of which would endanger and cause irreparable damages to the permanent interests of the country
- Classified information level **"SECRET"** is information, unauthorized disclosure of which would cause exceptionally serious damages to the vital interests of the country.
- Classified information level **"CONFIDENTIAL"** is information, unauthorized disclosure of which would cause serious damage to the important interests of the country.
- Classified information level **"RESTRICTED"** is information, unauthorized disclosure of which would cause damages to the work of the national and local authorities, and/or of legal entities which are significant to public security, defence, foreign affairs and security and intelligence activities.

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.

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

80 Article 9, Law on Classified Information, Official Gazette of the Republic of North Macedonia no. 275/2019

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

3.4.2 Access to information about intelligence sharing and exchange

Intelligence services have an obvious need to share information[81] with domestic and foreign partners. As most current security threats have a transnational nature, a service that simply collects intelligence information without sharing it is not performing its duty or warning others about the security threats it has detected.

Sharing and exchanging information, and cooperation with foreign services is one of the most sensitive and secret areas in the work of intelligence services. Therefore, it is understandable that services closely guard information related to or arising from these relations. The potential damage caused by unauthorized or unintentional disclosure of information by a foreign partner should not be rejected lightly. Besides the obvious implications to the privacy and personal safety because of disclosing certain types of information, there is also violation of the trust of foreign services that can lead to termination of the cooperation and its benefits. Therefore, it is essential for oversight authorities to adopt relevant security procedures and act with the utmost professionalism when handling information arising from the relations or referring to relations with foreign partners[82].

Although there is broad consent that sharing and exchanging information is required for increased security, the recent expansion in the exchange of information between different security and intelligence services within a country, and across borders, are raising a number of problems and risks that require close management and oversight. These are just a few examples:

- law enforcement and intelligence services may undertake operational activities based on shared information that is not verified, leading to poor allocation of limited resources and operational failure;
- information shared may be disclosed in subsequent legal procedures,
- the dissemination of insecure and/or irregularly obtained information may cause damage to the credibility and the image of a service;
- individuals are also exposed to a greater risk of violation of their rights, especially their right to privacy. They cannot challenge the accuracy of the shared information because oftentimes they are not even aware that information about them has been shared across agencies and across countries.
- risks for oversight authorities involve mainly new limitations to their capabilities of understanding which information is shared and how this exchange takes place.

To conclude, intelligence cooperation and exchange has become today so important that without information about it, parliamentary oversight committees have an incomplete view of activities involving their own state's agency. Getting more information about international

81 Hans Born, Aidan Wills (2012): Overseeing Intelligence Services: A Toolkit, The Geneva Centre for the Democratic Control of Armed Forces (DCAF), Geneva, pp. 129-147 https://dcaf.ch/sites/default/files/publications/documents/Born_Wills_Intelligence_oversight_TK_EN_0.pdf

82 Hans Born, Ian Leigh, Aidan Wills (2015): Making International Intelligence Cooperation Accountable, Norwegian Parliamentary Oversight Committee, DCAF Centre for Security, Development and the Rule of Law, p. 151

cooperation (or even being exempt from the third-party rule) is nowadays an endeavour of many oversight bodies in Europe.

› RECOMMENDATIONS FOR MITIGATION OF OBSTACLES FOR ACCESS TO INFORMATION EXCHANGE[83]

- Oversight authorities must identify the most important aspects of cooperation between national intelligence services and foreign partners.
- There should be at least one external oversight authority that has full access to information owned by intelligence services, including information from international intelligence cooperation, or relating to international intelligence cooperation, which is considered relevant for the fulfilment of its jurisdiction.
- The third-party rule (or the originator control principle) should not be permitted to override statutory provisions grating oversight authorities access to information necessary to fulfil their mandates. Parliamentarians should consider the option of making the legislation explicit that access to information by oversight authorities is not constrained by or subject to the third-party rule.
- The option of including a clause in the agreements that intelligence services conclude with foreign partners stating that cooperation may be subject to scrutiny by a certain oversight authority, should be considered.
- The legislation should allow oversight authorities to hire technical experts (undergoing a security check), who can help them in understanding and assessing intelligence issues, including cooperation and exchange of information with foreign partners; additional resources should be allocated to oversight authorities to ensure the hiring of such experts.

Besides promoting increased transparency by services, the oversight authorities should also release information about their work in overseeing international cooperation among intelligence services. Publishing such information is important for educating the public on how international intelligence cooperation is regulated, and for demonstrating to the public that national services' relations with foreign partners are evaluated. This role of oversight authorities is becoming even more significant in countries where aspects of international intelligence cooperation caused allegations over serious crimes. When drafting reports on thematic investigations or on investigations of specific cases/incidents related to international intelligence cooperation, oversight authorities should aim to produce a public version of the report, while keeping secret the enlarged version containing classified findings and recommendations[84].

3.4.3 Use, management and protection of personal data

The rapid development of information technology has increased dramatically the capacity of state agencies to collect and process personal data. This has created an important challenge:

83 Hans Born, Ian Leigh, Aidan Wills (2015): Making International Intelligence Cooperation Accountable, Norwegian Parliamentary Oversight Committee, DCAF Centre for Security, Development and the Rule of Law, pp. 152-155

84 Hans Born, Ian Leigh, Aidan Wills (2015): Making International Intelligence Cooperation Accountable, Norwegian Parliamentary Oversight Committee, DCAF Centre for Security, Development and the Rule of Law, p. 156

how to protect personal data subjects[85]and minimize the risks of accidental or unlawful access, destruction, loss, change of their personal data. Intelligence services should apply specific techniques and organizational measures in order to ensure (and also prove during oversight) that the personal data processing is conducted in compliance with the law, their quantity/ or volume is kept at minimum levels and safeguards against misuse and abuse are incorporated in the process. Personal data protection must be ensured by design and default within the processing process.

The technical and organizational measures for personal data processing should especially incorporate (but not limit to):

- The use of pseudonyms and encryption of personal data;
- The ensuring of continual confidentiality, access control, integrity, availability and resilience of processing systems;
- Capability for timely reestablishment of the personal data availability and access in case of physical or technical incident;
- A process of regular testing, assessment and evaluation of the effectiveness of technical and organizational measures, for the purpose of guaranteeing the security of personal data processing.

Different country's experiences show that the weakest link in IT security relating to personal data processing is the human aspect. To mitigate risks, intelligence services should limit the number of employees who have access to personal data to those authorised and properly trained for this.

Different country's experiences show that the weakest link in IT security relating to personal data processing is the human aspect. To mitigate risks, intelligence services should limit the number of employees who have access to personal data to those authorised and properly trained for this.

- **Confidentiality** means that access to information containing personal data can be provided only to persons who have the proper authorization by the controller (in this case the intelligence services). The authorization is issued by the responsible person with the controller, on the 'need to know' principle. Moreover, for the purpose of ensuring a full and clear division of duties and responsibilities, there should be a record of persons authorized to process information that contains personal data.
- **Integrity** or accuracy means that information containing personal data, owned by security-intelligence services, is accurate, complete and updated.
- **Availability** means that systems and devices used for personal data processing are designed in a way that they perform their function when necessary and only for the purposes they have been procured or designed for.
- **Authenticity** of IT security is a measure ensuring that only the authorized persons can enter and have access to the systems that include information containing personal data. This element of IT security enables relevant assumptions on the establishment of clear division of duties and responsibilities within the intelligence services, thus enabling the establishment of an information-auditory trace by registering every access and log (log management system).

85 Personal data subject is an identified natural person or a natural person who can be identified through a specific information, whereas a natural person that can be identified is a person whose identity can be established directly or indirectly, especially on the basis of an identifier such as name and surname, birth registry number of the citizen, location data, identifier over the internet, or on the basis of one or more features that are specific for his physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **Non-repudiation** of IT security is achieved in the process of digital certification. It includes the encryption of information by using specific encrypting tools, whereas the communication over the internet is digitally signed by the sender of the information.

FUNCTIONS OF IT SECURITY IN PERSONAL DATA PROCESSING

Prevention encompasses activities that intelligence services should undertake prior to the establishment of processes or systems that will serve as platforms for personal data processing. This function incorporates at least the following:

- Planning in detail the technical and organizational measures aimed to ensure secrecy and protection of personal data processing;
- Define the categories of personal data to be processed and of personal data subjects;
- Issue authorizations and conduct training for staff conducting personal data processing;
- Create and manage records for staff authorized to conduct personal data processing;
- Define timelines for deleting different personal data categories; and
- Designate an officer for personal data protection.

Maintenance incorporates activities that succeed and serve as support to the preventive measures:

- Regular update of documents describing the technical and organizational measures that ensure the privacy and protection of personal data processing;
- Update the use of technical and organizational measures;
- Periodic controls by the officer for personal data protection, ensuring the alignment of operations with regulations;
- Trainings for employees on personal data protection;
- Testing of the IT system after applying any changes, to check if secrecy and protection of personal data processing are ensured; and
- Internal control of IT system and IT infrastructure.

Reaction incorporates activities undertaken in case of a security incidents, as an anomaly that affects or could affect the secrecy and protection of personal data, i.e. expose information containing personal data. This includes:

- Reporting, reaction and rehabilitation of the incident;
- Recording of the incident and measures that were undertaken for its rehabilitation; and
- Measures that have been undertaken to avoid a repeat of the incident.

4

COMMITTEE IN ACTION: THE OVERSIGHT TOOLS

The oversight tools available to parliamentary committees are diverse, but their 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 them to reveal, explain and justify for their actions.

Committees' oversight activities are independent from the plenary or from the legislative schedule. Committees 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 members' decision.

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 deeds signalled 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 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 or not as independent, isolated activities. Different oversight tools are better suited in different stages of the oversight process.

1. Getting information and acquiring a good understanding of the intelligence sector is achieved though reports, consultative hearings, and field visits.
2. Oversight hearings, field visits, 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.
3. 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, in a democratic state all government departments are obliged to report to parliament and public[86]. 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 if taxpayers are receiving value for money. Intelligence services are not excluded from this practice[87].

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[88] of intelligence services are the most common type of reporting. There are many examples of intelligence services that regularly, most usually annually, publish activity reports[89] providing comprehensive and useful information for oversight, without compromising national security Sometimes, the text that is made publicly available does not necessarily contain all the information that was initially provided to the parliament, 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 competencies of the oversight body to whom the report is addressed to. 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, the threats to national and regional security, and oversight (substantial and financial) provisions.

- The length can vary from 20-30 pages (in Netherlands, Czech Republic or Croatia) to a very detailed in-depth report (Australia ASIO Annual Report 2019-20: 160 pages).
- The content[90] may cover, without divulging sensitive details: the annual objectives

86 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.

87 Hans Born, Aidan Wills (2012): Overseeing Intelligence Services: A Toolkit, p. 57 https://dcaf.ch/sites/default/files/publications/documents/Born_Wills_Intelligence_oversight_TK_EN_0.pdf

88 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.

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

90 See Annex D for examples of information contained in these reports

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.

Special reports are a supplement to the general yearly reports, and they are usually 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 in targeted hearings and inquiries of oversight bodies. The special reports are produced by the intelligence service, or they are based on research carried out by legal and 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 handicapping to effective oversight as too little information.

› 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, 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)[91].

91 Intelligence and Security Committee of Parliament (2017): UK Lethal Drone Strikes in Syria, p. 1-4

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 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 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[92].

Oversight hearings aim to obtain evidence or in-depth explanation on a specific matter. They are an effective tool for uncovering possible wrongdoings, misadministration, corruption or abuse of power, and for determining if there are grounds for impeaching a government official. Government officials are invited to provide information and respond questions in their area of competency. In most countries, laws and rules of procedure stipulate the obligation of the summoned officials to present themselves 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 finalize 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
- On rare occasions, if the topic of the hearing is very sensitive for national security, there is limited or no communication to the press and the public about the content of discussions or even about the occurrence of the event.

92 See for example the public debates on the Law on Interception of Communications in Macedonia – from 2012 (organized by the Committee on European Affairs) and 2018 (organized by the Committee on Security and Defence).

- 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 lawmaking, 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 taken also by a majority 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: government officials including 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 **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 satisfactory evidence and information on the subject of their investigation, or if they indicate that a matter needs further, more indepth investigation, the committee may propose the plenary to set up an inquiry committee, with a specific mandate. In rare cases, permanent committees can initiate themselves inquiries, 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 is their effectiveness is in pursuing government accountability; they may also add public pressure towards the implementation of parliament recommendations.

› MONTENEGRO, LAW ON PARLIAMENTARY OVERSIGHT IN THE AREA OF SECURITY AND DEFENCE/2010

Article 8. Consultative hearings

Consultative hearing shall be organised and carried out for the purpose of collecting information and professional opinions required for the work of the Committee, and particularly with regards to proposed solutions (development of laws, secondary legislation, or election of candidates); in addition to representatives of state authorities, experts and representatives of non-governmental organisations may be invited to facilitate qualitative preparation of the Committee for conduct of parliamentary oversight.

The Committee may engage experts in the capacity of consultants.

Costs incurred by engagement of experts as well as the wages for their work shall be paid in accordance with the act and in the amount established by the Administrative Committee.

The Committee shall submit the report on the findings of the consultative hearing to the Parliament.

Article 9. Control hearings

Control hearings shall be organised and carried out for the purpose of obtaining opinions and collecting information under the responsibility of the Committee and in case there is a need to eliminate ambiguities, dilemmas, principle-related disputes or clarify current disputable issues in carrying out of the policy and law and other activities of the Government and state administration authorities in the area of security and defence.

The Committee shall decide on control hearing by majority votes of all members.

Responsible representatives of the Government or other state administration authority, as well as other persons whose presence is required for clarification of the subject matter shall be invited to the meeting.

In the course of the control hearing, the Committee members may put questions to the person summoned to hearing for the purpose of clarifying specific matters.

Experts from specific areas may be invited to control hearing for the purpose of professional clarification of specific dilemmas and ambiguities as to facilitate qualitative preparation of the members of the Committee to conduct the parliamentary oversight.

After the control hearing is completed, the Committee shall produce a report and submit it to the Parliament which might disclose a summary and may propose relevant measures or conclusions.

Article 10. Parliamentary inquiry

The Committee shall initiate parliamentary inquiry if:

1) findings and conclusions of the consultative or control hearing show that it is necessary to consider the situation in respect of specific issues;
2) it is necessary to consider specific issues of public significance or collect information and facts on specific occurrences and events related to the policy and work of security and defence agencies;
3) findings and conclusions could be the base for the Parliament to decide on the political responsibility of holders of public functions or undertaking other actions under its responsibility.

Article 11. The procedure of consultative and control hearing and parliamentary inquiry shall be regulated by the Rules of Procedure of the Parliament.

4.3 FIELD VISITS

Field visits are powerful tools of oversight, for they offer members of parliament the opportunity to access first-hand information about the work of the services, engage with larger number of intelligence personnel than in parliamentary hearings, and check premises, technical equipment, and files.

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 in an explorative mission on territories it doesn't fully know, understand or control. The risk of losing its focus and getting derailed from its oversight objective is high. Therefore, the need to rely on expert staff support is more obvious in field visit than in other oversight activities.

Clear procedures are another prerequisite for successful field visits. Committee Rules of Procedure should clearly detail responsibilities and steps in implementing a field visit, allowing for a smooth and efficient decision making in all its stages.

Field visits can be analysed following three main phases: preparation, implementation and post-visit follow up. Each stage of this process will be different - depending on whether the visit is organised as a proactive oversight activity (announced well in advance, eventually included in the annual programme of the committee), or, if it is a reactive visit to carry out an investigation of some specific allegation or incident. However, some common principles inspire the organisation of field visits in all circumstances.

4.3.1 Preparation

Good preparation and proper planning are essential to reduce the risks of failure, which range from causing conflicts with the services, missing the scope of the visit or having strife within the visiting team. "Perfect planning prevents poor performance"[93]. A good preparation of the visit has a few distinctive steps:

Definition of the visit, objectives and priorities

The committee must discuss and develop a common position on what should be the goals and the priorities of the visit (e.g. a better understanding of the functioning of the services, contacts with high ranking officials and staff, controlling the legality of activities, building up mutual confidence, investigating media allegations against the service or citizens' complaints etc.).

- The objective and the priorities of the visit need to be compatible with the mandate of the committee. They need to be carefully defined, with the support of committee staff with legal expertise.
- Supporting staff should be involved from the very early stages.
- Not all visits can be planned far in advance and with a general objective such as improving the understanding of intelligence processes. Sometimes, visits are organised urgently after major incidents, complaints or allegations by citizens, politicians or media. These field visits require even better preparation, in order to avoid oversight failures and mitigate the risk of over-politicisation of oversight or of compromising possible judicial investigations.

93 Belgian intelligence review committee

Prior discussions

The next step in the preparation stage consists in engaging in communication with the ministers and heads of services about the committee's intention to organise a field visit, its objective and the context that led the committee to decide on the visit. Discussions will cover the location, the timing and the subject of the intended visit.

- This step precedes the actual planning of the visit and is important for detecting possible obstacles and eliminating potential animosities.
- The heads of the services may, at this point, already provide the committee with relevant information and documents, to inform the committee about relevant aspects of the visit.
- For security reasons, it is necessary to clarify and agree on how committee members get access to the facilities of the services.
- The issues discussed and agreed upon should be written down to avoid confusion and misunderstandings during and after the visits.

Choice of the sites and items to be visited

The committee decides on the site to be visited (headquarters of a service, local or technical installations, etc.) and on the specific areas that should be visited or consulted (such as operational rooms, archives, IT and databases, contact with staff).

- The choice can best be made after the general briefings given by the services that should include localisation of the facilities, even if some are classified information.
- A specific regime must be granted for specific facilities such as safe houses of which the secrecy is the reason of their existence. Normally, the committee has no need to know these localisations, but an agreement can be made with the service that all such facilities must be registered in a dedicated file, which can be consulted by the committee in case of major incidents.

Planning and organisation of the field visit

- This step refers to all practical and logistical preparations (timetable, execution time, etc.).
- The committee should establish a division of tasks and a role description for the participants (head(s) of the visiting team, rapporteurs, etc.).
- The committee should decide on what kind of report is to be made (formal of not), and what other formal documents the service should be asked to prepare.
- It is always recommended to prepare a number of questions, both of general character and specifically related to the visited site. Frequently asked questions refer to how the activities of the facility are planned, monitored, documented.
- Finding out about the internal control mechanisms and the persons responsible for them are very important in any field visit that looks into legal norms and the registration of operational activities.
- It is useful to discuss scenarios for the visit and the committee reaction to them. Especially "worst case scenarios" should be considered and mitigated. It can for example happen that access is denied, certain information is refused, strong discussions start with the service representatives, the committee members don't agree among themselves, visiting procedures are violated, etc.
- In some cases, if the committee counts a large number of members, or if the objective of the visit is very narrow, it might be practical to decide on a small visiting team that receives a mandate from the committee and reports to it. The procedural details of such an

arrangement must be very clearly spelled out in the Committee Rules of Procedure. It is important to have political representation from all major parties, in order to ensure the legitimacy of such sub-committee.

- Agree with the service on a point of contact, e.g. the commanding officer (CO) of the site.

4.3.2 Implementation

Access to the visited site and start of the visit

- The members of the visiting team should produce identification, and if necessary, their security clearances. Providing a copy of the documents is highly recommended.
- An explanation of the mandate and purpose of the visit to the staff receiving the committee is needed. Announce the requested items of the visit, such as the access to files and personnel, and the order in which the committee wants to proceed.
- An unannounced visit usually requires prior general approval of the minister in charge (as for many parliaments "unannounced" actually means the minister is informed 24-48 hours in advance). The general written approval of the minister or head of service gives a formal order to the members of the service to receive and cooperate with the visiting committee. It can take the form of a letter of access.

During the visit

- After the introductions it is common to invite the Commanding Officer to explain the missions and activities of the personal on the site. The visiting team members start asking the prepared questions.
- The preparation of the visit should have indicated what (internal and external) control tools are foreseen in the law or regulations to allow the verification of the issues investigated by the committee (such as inscriptions, logbooks, ICT login lists, personal staff lists, clearances). The committee may ask to see these data and registries; and engage in a dialogue with those responsible about the situation and the challenges faced in internal control.
- Members should not only ask for explanations but invite the Commanding Officer to show them examples of files, data and reports and if possible, inspect some data.
- When permitted by the CO, engage with executive staff and ask some questions on their concrete activities.
- Make sure that discussions or findings are systematically being put down in writing/ recorded by the rapporteurs.
- Remain objective. Unbiased oversight, even in complex and potentially conflictual situations, must be careful to record both the negative and the positive findings. Even when it seems evident that services comply to legal standards, it is necessary to write this down in reports so it remains a point of reference and comparison for future oversight activities; it might be useful to give a quote, positive or negative, on every item of the check list or questions list that guide the discussion.

Attitude during the visit

- It is usually more productive if committee members refrain from expressing their judgments of the situation as clear statements. Even if they have strong opinions, it is better to formulate these as questions, inviting further discussion.
- It not recommended to go into political of strategic discussions, certainly not amongst

members of the visiting team themselves. It is better to focus on the activities of the service: what are the proceedings, the outputs and outcomes, how intelligence is produced, what are the concrete rulings, how information is registered, controlled, archived.

End of the visit

Explain the follow-up to the CO and/or to his staff (reports, feedback, etc.). Summarise any agreements made during the visit, e.g. about the reporting or complementary information/ documents that will be sent to the visiting team.

Debriefing

Shortly after the visit, ideally the same day, it is recommended to organise a debriefing of the visit with the visiting team and/or the whole committee.

4.3.3 Post visit follow up

Reporting

The rapporteurs should submit a draft report to the visiting team and/or the committee as soon as possible. Specific attention must be given to classification levels and the dissemination of the report outside the committee. The report should include the opinion of the majority of members, but also mention minority opinions which might dissent.

- It is useful to distinguish findings: matters that need further investigation, possible consequences and recommendations, implications for future policy/legislation/budget.
- Recommendations should be divided into short-time, medium-time and long-term ones. They can also be distinguished according the authorities they concern, as in the following exemplifying table.

ITEM	FINDINGS	ACTIONS TO BE TAKEN /RESPONSIBLE AUTHORITY	TIMEFRAME
Surveillance of radical groups	1. According to legal mandate	None/ Parliament	–
	2. Absence of operational collection plan	Write collection plan/ head of service, approved by minister	6 months
	3. Minimal instructions for personnel	Develop formal Instructions/ head of service	1 year
	4. No findings of illegal practices by operational personnel	None/	–

Feedback

The responsible minister and the director of the visited service should receive a proper feedback, including conclusions and recommendations, and a request to report back on how recommendations are implemented.

The above table can be completed with a follow-up column, on what is realised and what not.

Evaluation

After one field visit or after a series of visits, an evaluation can be made by the committee (or by an external expert /parliamentary body) in order to adapt the proceeding and methodology if necessary.

Broader reporting

At some point - and perhaps at another level of classification - a broader report can be made to the whole Parliament and/or to the public.

› 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 well announced in advance, on 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 eventually that 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 with the objective and topic of the field visit) and that they cover physical access to the sites and facilities.
- Ensure the services understand the "need to know" principle for the specific oversight mandate of the committee, including the legal authority of the committee and the legal foundation for the committee oversight mandate.
- Leave the most sensitive sites (like interception facilities) for a later stage, when the committee has acquired a good understanding of the overall picture, so that they know better what and how to ask.
- A good 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. 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, similarly to a testimony in a court of law and with the same consequences for failure to provide the truth. However, these investigative powers can be employed **only** in relation to the immediate matter of inquiry and their duration is limited in time, by the mandate of inquiry.

Parliamentary Rules of Procedure 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 organisation 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[94] (exceptions are met in Germany, Belgium, Netherlands, Canada or 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 timeframe 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 asses 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 the 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

94 In 2007 a review of parliamentary oversight tools in 88 parliaments conducted by IPU has found that only in 13 parliaments standing committees can lead inquiries, always with the permission of the plenary.

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 co-operation 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 scrutinised, the fact that a person is a private person and does not occupy any public role should not exempt such person from being summoned to appear in front of a Commettee.

› WHAT SPECIAL INVESTIGATION POWERS MAY COMMITTEES HAVE?

In the German Bundestag The Defence Committee has an outstanding position because its settling is provided for in the constitution and it is the only committee which may declare itself to be a committee of inquiry (Art. 45a, para (2) of the Basic Law). 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 evidence[95]. 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[96]. The judge can also order a search for the seizure of items requested by the inquiry committee as evidence[97].

95 Law on Inquiry Committees, section 21, 27, and 29
96 Ibid. Section 27 (2)
97 Ibid. Section 29 (3)

- The federal government is required to grant the necessary authorization for the examination of office holders.[98]

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[99].

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 failure to provide the required information (Art.22), prescribing fines that can go up to 2 000 EUR for employees and to 20 000 EUR for legal entities.

In practice, inquiries are an oversight tool that are **rarely used**, often as a last resort[100]. Few parliamentary inquiries have delivered satisfactory results, at least in the area 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 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; 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 2016, WikiLeaks released over 2,400 documents which it claims are from the investigation.
- In France and Belgium, the respective national parliaments created a special inquiry committee after the terrorist attacks of 2015 and 2016.
- In 2006, the Romanian Senate established an ad hoc inquiry committee that, over two years, investigated the existence of CIA secret detention sites on national territory. The report was kept entirely secret except for its conclusions, which categorically deny the possibility that secret detention facilities could be hosted on Romanian soil. However, these conclusions were contradicted by the "Fava Inquiry" of the European Parliament (2007) and by the ECHR case Al Nashiri v. Romania (2018).
- In Bosnia-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

98 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. https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html Further analysis of special legislation would be needed to clarify whether former civil servants are obliged to testify, but it seems so.

99 Art. 6 of the 1958 Law on the Functioning of Parliament

100 Most parliaments create inquiry committees only a few times during a legislative term. For example, the House of Representatives in the Netherlands has created only 10 inquiry committees in the last 3 decades. https://www.houseofrepresentatives.nl/how-parliament-works/parliamentary-inquiry

launch an investigation. This never happened.

- In 1994, the 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 organisation 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[101].

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.

101 https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFl

5

OUTSIDE THE SECRECY CIRCLE: INTELLIGENCE OVERSIGHT AND THE PUBLIC

Accountability is a chain of relationships that ultimately leads to the public. Through elections, the public has delegated its power to its representatives, but it preserves the right to know how state bodies protect national interests and spend public funds. The value of oversight mechanisms relies not only on how they manage to foster intelligence accountability, but also in their own transparency and openness to the public.

The establishment of specialized intelligence oversight committees in the majority of democratic parliaments has not necessarily led to increased public accountability and transparency of intelligence sectors. Instead, it is the intelligence oversight bodies that are profoundly influenced by the norms of secrecy derived from security and intelligence services. A number of studies point out a trend towards the 'secretization' of oversight, as concerns for secrecy prevail over the responsibility to inform the public about intelligence accountability. In many parliaments committee meetings are closed as a rule, their meetings, agenda items and conclusions are kept secret and none of their reports are disseminated to public.

For the public, oversight done in secrecy is oversight undone. The lack of an open record in denouncing mistakes, abuses, individual or systemic problems in intelligence will end up by undermining the credibility of parliament as competent supervisor of the public interest and as vigilant defender of individual rights. A protracted silence on intelligence matters will make committees, and parliament in general, look ineffective and even compliant in relationship with intelligence.

For these reasons, intelligence oversight committees need to inform the public about their work; they must reach out to media, civil society and other independent oversight bodies, build up alliances and partnerships dedicated to improved democratic accountability. Specific strategies may be needed to reach marginalized communities, which are more likely subject to human rights violations and abuse in the exercise of special powers of security and intelligence services.

5.1 PUBLIC REPORTING

Parliamentarians represent their constituents and are accountable to the public for their parliamentary activity. It is impossible for the public to monitor the performance of their representatives if their work takes place exclusively behind closed doors.

Given the secret nature of intelligence technique and operations, it is undeniable that full transparency of oversight is neither possible nor desirable. Committees must reconcile the democratic requirement for transparency with the equally important constraint of protecting classified information. If the laws are clear in defining what is classified information and what is information of public interest, and if the communication between the services and the committee is effective, based on mutual trust and respect of the procedures, the committee can easily distinguish what can be published and what should be kept in the 'ring of secrecy'.

The committees have several ways to report to the public, the most frequently used being:

- Committee press releases – usually drafted by committee staff and endorsed by the committee chairperson or by all members (if the subject is politically sensitive),
- Parliament's Public Relations Office – they maintain the communication with the journalists accredited to the parliaments; they usually employ specialists in communication who can assist committees in drafting press releases or even establishing a communication strategy

- Committee reports on legislation and oversight (unclassified versions) are published on parliament website.
- Interviews given by individual members to the press.

In the aftermath of Snowden revelations from 2013 about mass surveillance programmes carried out by several governments, there was a significant effort of intelligence agencies to improve communication, exchanges and cooperation with oversight bodies and especially with the large public. In many countries intelligence services today publish **Annual Activity Reports**. This is a sign that the intelligence community is aware how important public support, legitimacy and credibility are in a democratic society. Often, these activity reports give quite detailed information about how the service was overseen by the parliament[102].

The Annual Activity Report of the intelligence service is usually submitted to the Parliament before being published. The intelligence oversight committees analyse the report and discusses with the service on eventual issues that need clarification. Then, the Report is presented to the plenary and the public. The plenary discussion of the annual activity report of the service is a common exercise of transparency for oversight committees – in some parliaments is the only occasion when the intelligence oversight committees express publicly their general assessments of intelligence activities.

Intelligence committees issue their own annual activity reports. Most often they have the legal obligation to submit this report to the governing body of the Parliament, which has the discretion to make the report public, once the text is redacted to take out sensitive information. The same procedure is applied for ad-hoc oversight reports of the committee. There are formal or informal procedures by which agencies must be consulted about material which they believe should not be made public.

› WHAT ARE THE REPORTING PRACTICES IN DIFFERENT PARLIAMENTS?

Recognizing that the credibility of oversight relies on communication with the public, the legal framework on the mandate and powers of the Romanian intelligence oversight committee was amended in 2017. The previous provision that stipulated that "all information about committee work is classified information" has been replaced with a re-affirmation of the committee responsibility to protect classified information, according to relevant laws[103]. In the spirit of these regulatory changes, the committee has become more active and started to publish information about its activities on the parliament website. While no information whatsoever was available about the committee activities in the last decade, in 2017 the committee held 45 sessions, followed by 30 sessions in 2018, initiated investigations and hearings and made frequent press releases.

In the UK the Investigatory Powers Commissioner and the Intelligence and Security Committee of Parliament (ISC) must report as soon as reasonably practicable after the end of each calendar year. The Prime Minister can exclude material from a report if publication would be prejudicial to the continued discharge of the functions of the agencies.

Intelligence oversight committees from the parliaments of Italy, France, Germany, Sweden and UK have a legal obligation to publish annual activity reports. The length of these reports varies from 93 pages (France) to 14 pages (Germany), they refer to statistical data on committee activities (like the number of sessions and hours of work), oversight methods, inter-institutional dialogue, and recommendations[104].

102 It can happen that the intelligence service reports on oversight activities while the intelligence oversight committee is completely opaque to the public. This is not putting the parliament in a favourable light.

103 HP no 85/October 2017, Art I(5).

104 European Union Agency for Fundamental Rights (FRA) Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU, Volume II: Field Perspectives and Legal Update, 2017, p. 87 and 164

5.2 ASSESSMENT OF OVERSIGHT

The main problem in evaluating the committees' oversight performance is the fact that little information is available about their activities. A second challenge is the absence of clear performance criteria. The most important factor to follow is the impact of oversight on the activities of the services. Oversight committees should keep track records of their findings and recommendations and introduce a follow-up system of these, with special attention to legal developments triggered by oversight.

A self-assessment is the first and the easiest choice for a committee that wants to evaluate the impact of its work on the overseen institution. A self-assessment offers some advantages to an evaluation conducted by external experts:

- Being a voluntary exercise, undertaken in the absence of external observers, it contributes to uninhibited debate on the strengths and the weaknesses of the committee;
- It avoids problems related to the access to classified information and the confidentiality of the committee work (which would be almost insurmountable for an outsider unless security is cleared)
- It is a good learning exercise, raising awareness and expertise on oversight principles, tools and good practices;
- Maximizes the possibility of using and linking the findings to national reforms.

Overall, a self-assessment has more potential than an external evaluation to contribute to institutional consolidation. However, it would require support from expert staff to conceptualize and facilitate the exercise (prepare questionnaires, semi-structured interviews with different stakeholders, focus group discussions etc.).

Instead of a self-assessment, an external expert or group of experts could be asked to conduct a performance audit of the committee's activity. Besides being more expensive, an external evaluation team would need to have /or to get security clearances and the legitimacy given by a mandate approved by parliament.

Self-assessment or external evaluation of parliamentary performance in intelligence oversight should refer to:

- an initial moment (baseline) on which information can be collected (indicators),
- the definition of the desired situation (target) and,
- a regular comparison of data during a certain period of oversight.

Most indicators that can be followed are qualitative, but even the quantitative indicators, that can be expressed through a number, must be carefully put in context.

Quantitative indicators may refer to the number of: committee meetings/ issues on the agenda/ regular reports received and debated/ special reports requested/ hearings/ visits in the field/ committee reports submitted to the plenary/ oversight activities initiated by minority groups/ complaints against the services/ interception mandates executed-rejected etc.

The availability of the above-mentioned statistical values in open sources represents an important indicator of parliament's transparency towards the public. The non-availability of such data about parliament activity should be questioned.

Qualitative indicators – reflect people's judgments, opinions, and attitudes towards a given situation or subject. They are most relevant in tracking trends in parliamentary performance,

because oversight is inherently complex, political, and qualitative in nature. Here are a few examples:

- The level of mutual trust, dialogue and collaboration between the committee, the relevant ministries and the intelligence services;
- The implementation of parliamentary recommendations by executive and security providers;
- The ministry/service responsiveness to requests for information and to hearings summons;
- The understanding of parliament's role and functions (within parliament and within the intelligence sector);
- Parliamentary awareness and understanding of relevant laws and procedures;
- Parliamentary attitude towards oversight and the political will to keep the government and the services accountable;
- The relationship developed by the committee with independent bodies mandated to play a role in democratic governance (Citizens Supervision Council, National Audit Office, Ombudsman, Personal Data Protection Agency etc.);
- The use of the media by MPs to convey positions and views;
- The use of independent expertise provided by civil society in the work of the committee;
- The existence of a human rights focus, in oversight activities;
- The Representativeness of parliamentary bodies, and use of strategies to be inclusive;
- The image of the parliament and the committee in the media;
- The image of the services in the media or public opinion;
- The transparency of the services (public reports, information provided based on law on free access to information of public interest, the existence of a public relations office etc.).

› WHAT ARE THE REQUIREMENTS OF EFFECTIVE OVERSIGHT?

Access: oversight and access to information must extend to personnel, sites and classified information that is necessary and sufficient for overseers to carry out their mandate.

Trust: oversight systems must be designed to maintain secrecy and the integrity of the intelligence process. Reliability is necessary to win the confidence of the intelligence services and to safeguard national interests.

Independence: oversight must be independent of partisan interests and of inappropriate influence by the intelligence services.

Authority: effective oversight depends on discretionary powers of investigation, including the power to compel testimony under oath.

Cooperation: members of Assembly committees must develop working relations with other oversight bodies both within the Assembly and outside - the People's Ombudsman, the Citizens Supervision Council, the Classified Information Security Directorate, the Personal Data Protection Directorate and the State Audit Office.

5.3 CIVIL SOCIETY ROLE IN SUPPORTING DEMOCRATIC INTELLIGENCE OVERSIGHT

Media, academia and think-tanks, as well as a wide range of civil society organizations (CSOs) focused on security sector and/or human rights issues, are providing public oversight of intelligence issues. In recent years, after the Snowden revelations, the interested public has become aware of things well-known in international politics: secret services have the capacity to invade the private informational space indiscriminately and massively. This new-found awareness has led to the mobilization of civil society organizations that are engaging more attentively and vocally in intelligence and security oversight, an exercise that gradually develops their expertise and credibility.

The public can exercise direct political pressure on both parliament and government, while the media play a key role in increasing public awareness, directing government attention to important topics and exposing misconduct in intelligence. Scandals can lead to investigation and result in reforms that improve the accountability and effectiveness of intelligence. MPS can raise attention through media and exert pressure on government to change policy and practice. Media pressure can be huge today, the faster and the most efficient way to put pressure on the government.

Public oversight must cope with the dilemma that those who know do not speak and those who speak do not know. Indeed, the rule of secrecy is a major problem for those outside the ring of secrecy to make pertinent observations on the security services but there are many examples where the press, academia, NGOs play an important role in the public debate on security. It is easier in countries where there is a tradition of discussing security, but also a culture of human rights that keeps attitudes in balance.

In younger democracies, it is the responsibility of oversight committees to contribute to the development of a political and civic culture and play the role of an interface between the closed world of the services and the public. They must help overcome the traditional, mutual suspicion between civil society and state institutions, especially those who operate in secrecy.

CSOs can provide independent analysis of legislation, policies and practices related to the work of intelligence. They might present different policy options, identify gaps in existing legislation and/or present comparative analysis of certain aspects of the intelligence. Members of CSOs are usually considering legislation and policies in a non-partisan way, from the aspect of protection of human rights and freedoms according to the international standards on good governance. They can also encourage public debate on priorities, policies and needs for legislation change. CSOs might advocate for inclusion of minorities in the work of the intelligence services or gender-sensitive services.

› WHAT ARE THE CONDITIONS FOR EFFECTIVE PUBLIC OVERSIGHT?

The effectiveness of public oversight depends on access to reliable information. Legal rules about the classification of information should reconcile accountability and transparency with reasonable secrecy, for example through:

- ***Freedom of information laws*** allowing members of the public access to government-held data;
- ***Classification timeframe,*** that clearly define what, when and how long information may be kept secret, including a designated timeframe for its de-classification;
- ***Whistle-blower protections,*** that allow intelligence personnel to reveal information that exposes misconduct to designated internal or external bodies without fear of punishment for violating their obligation to maintain confidentiality and obedience.

6

ANNEXES

6.1. ANNEX A: GLOSSARY OF TERMS

Accountability – a concept whereby one entity has the right to hold another entity responsible for the fulfilment of a collection of standards, judge on the fulfilment of its responsibilities and punishment if those responsibilities are not met.

Audit – independent evaluation of financial reports or consolidated reports and financial information, for the purpose of expressing an opinion regarding their credibility and impartiality, as well as their alignment with the accepted framework for financial reporting.

Classified information - material that a government body deems to be sensitive information that must be protected. Access is restricted by law or regulation to particular groups of people with the necessary security clearance and need to know, and mishandling of the material can incur criminal penalties.

Classification (levels of classification) - levels of classification are used to designate how sensitive certain information is. European institutions, NATO ad most European countries have four levels: Top secret, secret, confidential, restricted. The U.S government uses three levels of classification: confidential, secret and top secret. The levels of classification and their protection are proportional to the harm incurred to the national interests by unauthorized access or unauthorized use of the information.

Classification timeframe - define what, when and how long information may be kept secret, including a designated timeframe for its de-classification.

Communication – giving or exchanging information among people through speech, sound, light, written text, drawing, image, item or gestures, as well as technical process of sending, transmitting and receiving any type of speech, data, sounds, signals, written text, static and moving images, which serve for information exchange among people, between people and objects, among objects or management of any object with the help of a telecommunications system, internet protocol, voice over internet protocol, website and e-mail.

Competent authorities for implementation of measures for interception of communications for the purpose of protecting the interests of national security and defense - National Security Agency, Military Service for Security and Intelligence (within the Ministry of Defense), Center for Electronic Reconnaissance (for radio waves HF, VHF and UHF).

Competent authorities for implementation of special investigative measure – public prosecutor and judicial police.

Data – simple, isolated, unprocessed info-content that has certain significance. It is created and transmitted in a form that is understandable by a person (text, image, sound etc).

Electronic registry system – registry that automatically saves the record/log (hereinafter log), which replicates the performed activities of the recorded communication, in line with the Law on Interception of Communications. Automatic recording represents a systematic recording of logs, with less human intervention. The logs should be accessible and legible for the purpose of oversight and control.

Executive control – in a democracy the executive typically has two main control responsibilities over intelligence: (1) enabling the operational effectiveness of the services – through the

definition of overarching policies, priorities and budgets, the authorization of sensitive operations, the investigation of cases of suspected misconduct, and (2) the political responsibility to parliament and the public for ensuring an effective, accountable and legal conduct of intelligence services. Autonomously operating intelligence services often fall under the direct control of the executive, through the president or prime minister's office or a joint executive body such as a national security advisory board. Intelligence functions situated within institutions such as the military or law enforcement agencies are usually supervised by sector-specific ministries or departments, such as defence, justice or the interior

Hearing – a hearing is a proceeding before a court or other decision-making body, such as a parliamentary committee. Hearings aim to collect information, evidence, expert opinions or in-depth explanation that are need for a parliamentary committee to make informed decisions on legislation or other matters; government officials, independent experts and even private citizens may be summoned to a parliamentary hearing. In some countries, laws or rules of procedure make a difference between consultative (or legislative) hearings and oversight hearings.

Information – complex info-content (knowledge) and set of data that is logically linked.

Inquiries – an in-depth investigation of a matter of special interest. Inquiries are always conducted in the framework of a specific and narrow mandate that defines its topic, scope, and timeline; most often they are conducted by special ad-hoc committees. Inquiries are the most "aggressive" and effective investigative tool available to parliament: inquiry committees have investigative powers similar to those of courts and public prosecutors (subpoena powers). Their summoning powers extend to officials, citizens, public, and private entities; they often have the power to enforce their summons and to sanction those who fail to comply. Inquiries often examine possible governmental abuse, mismanagement, inaction, or incorrect action, or misconduct by politicians and civil servants.

Intelligence – process comprised of measures, activities and procedures undertaken for: collection, documentation, analytical processing of data and information, and their use for a certain purpose.

Intelligence sector – all security-intelligence services (intelligence-security community), special state entities and departments within ministries dealing with intelligence activity.

Internal control – rules, processes and organizational structures within an intelligence service that ensure staff perform professionally and effectively within the limits of their authority, in compliance with the law and with respect for human rights, including gender equality. Internal control is a function and a responsibility of management.

Intelligence sector control – the power to manage and guide the intelligence service; it is carried out by the intelligence service over itself (exercised hierarchically by management and by internal control mechanisms) and/or by an authorized ministry and its staff (executive control). It can incorporate internal oversight but doesn't include and cannot replace the external oversight.

Intelligence services – state organisations that collect, process and analyse information related to threats to national security, in order to produce and disseminate "intelligence" reports that inform decision makers. They often conduct missions and task clandestinely and have a legal mandate to use intrusive methods for information collection. They can be a fully independent agency, or a department in a ministry (such as defence, interior,

justice). Variously called: security service, intelligence service, intelligence agency, intelligence and security service.

Intelligence community – encompasses all state services and departments that conduct intelligence activities and work separately and together to support national security and prevent threats to national security in a country. In many countries intelligence community is not only a concept, but an organisational structure tasked to ensure the functional collaboration between intelligence services including the coordination of joint operative or informative activities; they may integrate information produced by different services to generate a coherent, consistent intelligence product, thus controlling the degree of overlap in intelligence, and ensuring complementarity, confirmation or invalidation of information. In the Republic of North Macedonia, the intelligence community is composed of: National Security Agency, Intelligence Agency and the competent intelligence unit for military security and intelligence within the Ministry of Defense, i.e. Military Service for Security and Intelligence (MSSI).

Interception and recording of telephone and other electronic communications – secret acquisition of the content of the technical process of sending, transmitting and receiving any type of speech, data, sounds, signals, written text, static and moving images, which serve for information exchange among people, between people and objects, among objects or management of any object with the help of a telecommunications system, internet protocol, voice over internet protocol, website and e-mail, by having access to the technical equipment of operators, and parallel creation of a technical record for the content of the communication, with a possibility for reproduction.

Intrusive methods for information collection – measures for information collection that violate, to a certain degree human rights guaranteed by laws and constitutions, especially the right to privacy. They are used for collection of evidence in criminal investigations by police and prosecutors (based on criminal procedure code), or for preventing threat to national security by intelligence services (based on statutory laws for intelligence services, national security or other special laws such as laws on interception of communication).

Logs – file or files that are automatically created, recorded or stored on the server in an electronic register, containing data on all performed activities, the subject that performed them, the phone number, the IP address or other technical identification, the start and end of the activity.

Means for interception of communications – electronic, mechanical or other technical means used to learn or record the content of any communication.

Measures for interception of communications – surveillance and recording of phone and other electronic communications; surveillance and recording of interiors, enclosed spaces and items; entrance in facilities, enclosed rooms and items for the purpose of creating conditions for the measure's implementation; surveillance and visual recording of persons in open space and public places; surveillance and audio recording of content of communications of persons in open space and public places.

Need to know principle – access to classified information is usually regulated through the "need to know" principle, which means that parliamentarians have access to strictly necessary classified information in the framework of their professional duties only. Even if a parliamentarian has all necessary official approvals, he or she should not get access to specific information unless he or she uses its prerogative of using the *needs*

to know principle. This principle aims to discourage free "browsing" of sensitive material or the misuse of classified information for personal use.

Officer for classified information protection – for efficient and coordinated execution of the rights and obligations related to classified information, in the state and local government bodies established in accordance with the Constitution of the Republic of North Macedonia and by law, legal entities established by the Republic or the municipalities , the City of Skopje and the municipalities in the City of Skopje and other legal entities appoint one or more officers for classified information protection.

Oversight – catch-all term that encompasses ex ante scrutiny, ongoing monitoring and ex post review, as well as evaluation and investigation.

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.

Secret surveillance – the monitoring and observing/listening to persons, their movements, communications (physical or electronic) and other activities, and the recording of such activities without their knowledge.

Special investigative measures/techniques – information collection measures infringing the right to privacy, employed secretly by law enforcement for collecting evidence in criminal investigations, and based on criminal law/criminal procedure code. In North Macedonia, the types of special investigative measures are prescribed in Article 252 of the Law on Criminal Procedure.

Special powers – authoritative functions intelligence services have to collect information, such as the power to intercept communications, to conduct secret surveillance, to make use of secret information and of undercover agents, the power to enter houses clandestinely, etc. Some intelligence services may have (in circumstances clearly defined by law and for deterring certain threats to national security) forms of police authority allowing them to search, arrest or detain people.

Supervision – oversight or monitoring of the operations of a certain segment in the functioning of an institution or a legal entity (ex: Personal Data Protection Agency supervises the section of personal data protection).

Telecommunications – each transfer of signs, signals, images, sounds, data of any nature, transmitted fully or partially by wires, electromagnetic, photoelectric or photo-optic system.

Vetting – vetting is intended to assure government bodies that the individual has not been involved in espionage, terrorism, sabotage or actions intended to overthrow or undermine Parliamentary democracy by political, industrial or violent means. It also assures the department that the individual has not been a member of, or associated with, an organisation which has advocated such activities or has demonstrated a lack of reliability through dishonesty, lack of integrity or behaviour. Finally, the process assures the department that the individual will not be subject to pressure or improper influence through past behaviour or personal circumstances[105].

105 UK government vetting policy at https://publications.parliament.uk/pa/cm199495/cmhansrd/1994-12-15/Writtens-4.html

6.2. ANNEX B: OVERVIEW OF MACEDONIAN LEGISLATION FOR PARLIAMENTARY OVERSIGHT

CONSTITUTION OF THE REPUBLIC OF NORTH MACEDONIA

Art. 68

The Assembly of the Republic of North Macedonia

[...]

- selects, appoints and dismisses other holders of public and other office determined by the Constitution and law;
- carries out political monitoring and supervision of the Government and other holders of public office responsible to the Assembly.

[...]

Art. 76

The Assembly sets up permanent and temporary working bodies. The Assembly may set up survey commissions for any domain or any matter of public interest. A proposal for setting up a survey commission may be submitted by a minimum of 20 Representatives. The Assembly sets up a permanent survey commission for the protection of the freedoms and rights of citizens. The findings of the survey commissions form the basis for the initiation of proceedings to ascertain the answerability of public office-holders.

LAW ON THE ASSEMBLY OF THE REPUBLIC OF NORTH MACEDONIA

Official Gazette of the Republic of Macedonia no. 104/2009

V. PARLIAMENTARY OVERSIGHT

Oversight hearings

Art. 20

(1) An oversight hearing is held in order to obtain information and experts' opinions from the area of competence of the relevant working bodies in relation to the establishment and the implementation of the policies, the implementation of the laws and the other activities of the Government and the state bodies.

(2) The oversight hearing is conducted by the relevant working body of the Assembly which can invite at its meetings authorized representatives from the Government or from other state bodies, and request from them information and clarifications regarding the subject of the oversight hearing.

(3) At the oversight hearing other persons can be invited that can give information regarding the subject of the oversight hearing.

(4) The invited authorized representatives have an obligation to be present at the meeting on which the oversight hearing is held.

(5) The Chairperson of the working body shall notify the President of the Assembly

on the holding the oversight meeting, after which he/she shall send a written notification to the Government. With the notification the President of the Assembly will request that the Government appoints authorized representative(s) for the subject of the oversight hearing.

(6) The Chairperson of the working body shall send a written notification to the authorized representatives of the Government or the state body, to invite them at the meeting of the working body at which the oversight hearing will be held, and notifies them of the subject of the hearing; he/she can also request the information, opinions and views to be sent in a written form at least three days before the holding the meeting of the body.

(7) Finances for holding of the oversight meeting shall be secured from the Assembly's finances within the Budget of the Republic of North Macedonia.

(8) The public shall be informed about the oversight meetings through the Assembly's website and the Assembly TV Channel.

Art. 21

(1) Initiative for holding an oversight hearing can be instigated by one member of the relevant working body.

(2) On holding an oversight hearing the working body shall decide with majority of the votes from the present members, and with at least one third from the total number of members.

(3) If 15 MPs file a written request for holding an oversight hearing, through the President of the Assembly to the Chairperson of the working body, then the Chairperson of the working body is obliged to convene a hearing.

(4) The President of the Assembly with the Vice-Presidents and the Coordinators of the Parliamentary Groups shall give a recommendation for holding certain oversight hearings, to the Chairperson and the members of the working body.

Art. 22

(1) During the oversight hearing, the members of the relevant working body and the MPs that are not members of the relevant working body can ask the authorized representatives of the Government or the state bodies invited at the hearing questions related only to the subject of the hearing.

(2) During the oversight hearing there can be a discussion with the invited persons that have the information only if it is necessary to harmonize or clarify concrete issues and facts.

(3) The relevant working body shall decide on the duration of the hearing, ensuring the participation of every member of the relevant working body in the debate.

Art. 23

(1) The oversight hearing shall be recorded phonographically and minutes shall be kept; while technical and other corrections shall be done in agreement with the person that has given a statement.

(2) The working body shall prepare a report from the hearing and shall submit it to the Assembly; the report shall contain the essence of the presentations and it may contain conclusions which shall be distributed to the Government of the Republic of North Macedonia.

(3) The conclusions from the oversight hearing shall be posted on the web site of the Assembly.

LAW ON THE INTELLIGENCE AGENCY

Official Gazette of the Republic of Macedonia no. 19/1995

II. OVERSIGHT OF THE WORK OF THE INTELLIGENCE AGENCY

Art. 9

The Parliament of the Republic of North Macedonia supervises the work of the Agency through an appropriate Committee (hereinafter: the Committee)

Art. 10

The Committee submits to the Parliament of the Republic of North Macedonia a report on the performed work at least once a year.

Prior to submitting the report referred to in paragraph 1 of this Article, the Committee shall be obliged to submit the report to the Director of the Agency in order to obtain his opinion, and in particular from the aspect of the protection of the confidentiality of certain parts of the report.

Art. 11

The Director is obliged to provide insight and to provide all information and data from the scope of the work of the Committee.

Information and data presented at a Committee meeting are considered a state secret.

Art. 12

The Parliament of the Republic of North Macedonia submits the conclusions regarding the report on the work of the Commission to the President of the Republic of North Macedonia and the Government of the Republic of North Macedonia.

LAW ON DEFENCE

(unofficial consolidated version)

Official Gazette of the Republic of Macedonia no. 42/2001, 05/2003, 58/2006, 110/2008, 51/2011, 151/2011, 215/2015, 42/2020, Decision of the Constitutional Court of the Republic of Macedonia no. 37/2002 (O. G. 73/2002) and no. 135/2002 and 155/2001 (O.G. 78/2002)

CHAPTER III: Authorities of Agencies of The State Power

Article 17

The Parliament accomplishes the following:

1) performs supervision on the realization of the authorities of the Government in the defense area and follows the preparations of the Republic for defense;

2) states an immediate military threat to the Republic;

3) declares beginning and finish of the state of war;

4) decides on the extent of the funds necessary for the defense;

5) approves the wartime budget of the Republic;

6) decides on joining and resigning from the collective security and defense systems;

7) ratifies international agreements which pertain to entering, transiting through or presence of armed forces of foreign countries on the territory of the Republic of North Macedonia for exercise, training activities, participation in peacekeeping, in NATO missions and operations and in the application of the right to individual or collective self-defense and operations for crisis management and cooperative security, as well as participation in those activities and operations of Army members and employees of the Ministry of Defense abroad;

7-a) ratifies international agreements relating to the establishment and stay of commands, headquarters and military units of international organizations on the territory of the Republic;

7-b) makes a decision to send a request to NATO for assistance in defense of the Republic;

7-c) decides on sending members of the Army and employees of the Ministry of Defense out of the territory of the Republic to participate in international operations;

8) adopt a National Security Strategy;

8-a) adopts a Long-term plan for development of defense capabilities;

8-b) adopts documents for the functioning of the Assembly in a state of war;

9) declares the Armed Forces Day;

10) passes conlcusions and resolutions regarding the defense system, plans for defense development, equipping and combat readiness of the Armed Forces.

The Government submits a report on the documents from Paragraph 1 of this Article, on request by the Parliament or on two-year basis.

In order to introduce herself/himself to the activities within the Armed Forces, a Parliament member may ask for a visit to its units, command posts and headquarters organized by the Ministry of Defense.

LAW ON INTERCEPTION OF COMMUNICATIONS

Official Gazette of the Republic of Macedonia no. 71/2018

IV. SUPERVISION AND CONTROL OVER IMPLEMENTATION OF THE MEASURES FOR INTERCEPTION OF COMMUNICATIONS

1. Supervisory bodies for implementation of the measures for interception of communications

Supervisory bodies

Art. 35

(1) Supervision over the measures for interception of communications being implemented by the authorized bodies as well as supervision over the operator and the OTA shall be performed by:

- the Assembly of the Republic of North Macedonia;
- the Classified Information Security Directorate;
- the Personal Data Protection Directorate and
- the Ombudsman.

(2) Supervision over the measures for interception of communications being implemented by authorized bodies as well as supervision over OTA shall be performed by the Citizens Supervision Council.

(3) Upon request of the supervisory bodies referred to in paragraph 1 of this Article, the OTA shall assist in the implementation of the supervision over the operators.

(4) The OTA, pursuant to the Law on Operational Technical Agency, shall autonomously or upon request of the Authorised Authorities perform expert supervision of the operator.

Obligations to keep an official secret

Article 36

(1) The persons in the supervisory bodies referred to in Article 35 and the experts referred to in article 39 of the present Law shall be obliged to keep as an official secret the classified information, including a personal data which they have come across during the performed supervision pursuant to a law.

(2) The obligation referred to in paragraph (1) of the present Article shall remain even after the termination of their function in the supervisory bodies, i.e. even after the end of their engagement or as expert for a period of five years.

Obligations for security certificate

Article 37

(1) The persons referred to in Article 36, paragraph 1 of the present Article shall be obliged to be in possession of a security certificate with an appropriate degree for access to classified information.

(2) The security certificate referred to in paragraph (3) of the present Article shall be issued within a period not longer than 30 days from the day of submission of the request in the manner and in a procedure specified with a law.

1.1. Supervision by the Assembly of the Republic of North Macedonia

Composition of the Committee

Article 38

(1) To perform the supervision from Article 35 of the present Law, the Assembly of the Republic of North Macedonia shall set up a Committee from the Members of the Assembly of the Republic of North Macedonia for supervision over the implementation of the measures for interception of communications (hereinafter: "the Committee").

(2) The Committee shall be composed of a President, four members, a deputy President and four deputy members.

(3) The President of the Committee shall come from the lines of the political party in the

Assembly of the Republic of North Macedonia in opposition having received most of the votes at the last parliamentary elections, two members and deputies of the Committee shall come from the lines of political parties in power and two members and deputies shall come from the lines of political parties in opposition in the Assembly of the Republic of North Macedonia.

Accreditation of technical experts

Article 39

(1) The Committee referred to in Article 38 of the present Law for the purpose of conducting effective supervision shall hire national and international technical experts in possession of the appropriate expert knowledge, which upon their accreditation as part of the Committee can actively participate in the supervision.

(2) The Committee shall soon after its establishment and no later than 50 days select 2 experts for permanent support and prepare a list, within 6 months, additional national or international experts that may be accredited as experts on a case by case basis for the time necessary to prepare, conduct and report on the technical result of the conducted supervision.

(3) Upon a request from the Committee, the Electronic Communications Agency, the Classified Information Security Directorate and the Personal Data Protection Directorate, an authorised body not subject to supervision and any other state institution shall provide expert support to the Committee for issues within their competence as specified by law when performing supervision pursuant to the present Law.

Purpose and manner of performing supervision

Article 40

(1) The committee shall perform the supervision referred to in Article 35 of the present Law in order to determine legitimacy of the implementation of the measures for interception of communications referred to in Articles 7 and 18 of the present Law, as well as the efficiency of the implementation of the special investigative measures.

(2) The Committee and technical experts accredited as part of the Committee when performing the supervision, for the purpose of establishing legitimacy of the measures referred to in paragraph (1) of the present Article, shall compare the data referred to in Articles 41, 42 and 43 of the present Law which are in possession, owned or generated by the authorised bodies, the OTA and the operators, as well as the effectiveness of the implementation of the special investigative measures.

(3) The Committee, at its session, for the purpose of determining the effectiveness referred to in paragraph (1) of the present Article shall consider the annual report of the Public Prosecutor of the Republic of North Macedonia for the special investigative measures which will be submitted by the Public Prosecutor of the Republic of North Macedonia to the Assembly of the Republic of North Macedonia, pursuant to a law.

Data requested from the operator when performing supervision

Article 41

The data in possession, owned or generated by the operator which shall be made available upon request of the Committee or that can be retrieved directly by technical experts accredited as part of the Committee during the supervision are:

- Logs on the time and the date of the beginning of the measure for interception of communications;
- Logs on the time and the date of the termination of the measure for interception of communications;
- Logs on confirmation of the activation;
- Logs on total number of positive confirmations executed in a given period.

Data requested from the OTA when performing supervision

Article 42

The data in possession, owned or generated by the OTA which shall be made available upon request of the Committee or that can be retrieved directly by technical experts accredited as part of the Committee during the supervision are:

- Anonymised court order and anonymised provisional written order;
- Logs on the number of the anonymised court order;
- Logs on time of initiation and termination of the implementation of the measure for interception of communications;
- Logs on the total number of implemented measures for interception of communications in a given period.

Data requested from the authorized bodies when performing supervision

Article 43

The data in possession, owned or generated by the authorized bodies which shall be made available upon request of the Committee during the supervision are**:**

- Anonymised court order and anonymised provisional written order and
- Documents relating to the initiation and termination of the implementation of the measure for interception of communications.

Manner of performing supervision

Article 44

(1) The Committee shall perform the supervision without prior announcement, when necessary and at least once within a three months period even in absence of majority votes.

(2) Once the supervision is completed, the Committee shall draft a report on the performed supervision, stating if there was legal or illegal activity i.e. whether there has been abuse in the actions.

(3) **In case** the report referred to in paragraph 2 of the present Article **determines legal action it** shall be submitted before the Assembly of the Republic of North Macedonia and the Committee shall inform the public.

(4) In case when the performed supervision determines irregularities or abuses in the procedure of implementation of measures for interception of communications as specified with

the provisions of the Criminal Procedure Law and the provisions of the present Law, as well as a violation of any ratified international agreement ratified pursuant to the Constitution of the Republic of North Macedonia, the Committee shall be obliged to:

- notify the competent Public Prosecutor within 24 hours;
- notify the competent authorities in case of data protection and human rights infringement;
- inform, where appropriate and without giving specific data, the Assembly of the Republic of North Macedonia;
- inform, where appropriate and without giving specific data, the public.

Reports of the Committee

Article 45

(1) The Committee shall submit annual report before the Assembly of the Republic of North Macedonia for the previous calendar year by the end of February of the current year, at the latest.

(2) The Assembly shall consider and adopt the report referred to in paragraph (1) of the present Article by majority of votes of the total number of members of the Assembly and shall give recommendations for the work of the Committee.

(3) When necessary and upon request of the Assembly of the Republic of North Macedonia, the Committee shall submit additional reports.

(4) The public shall be informed accordingly about the report referred to in paragraph (2) of the present Article.

Rules of procedure

Article 46

The Committee shall adopt Rules of Procedure for its work, regulating issues on the procedure and manner of work of the Committee as well as on the manner of hiring of technical experts.

1.2. Citizen Supervision Council

Appointment

Article 47

(1) With the aim of exercising citizen supervision over the legality of the implementation of the measures for interception of communications a Citizen Supervision Council (hereinafter: Council) is hereby set up.

Composition of the Council

Article 48

(1) The Council is composed of a President and six members assigned by the Assembly of the Republic of North Macedonia for a period of 3 years without a right to re-appointment

(2) The Assembly of the Republic of North Macedonia shall issue a public vacancy announcement to assign a President and six members out of whom three shall be experts, and three shall be representatives of non-governmental organizations (citizen associations) from the field of protection of basic human rights and freedoms, security and defense.

(3) A President and a member of the Council may be a person having fulfilled the following conditions:

- be a national of the Republic of North Macedonia,
- at the moment of issuing public vacancy announcement, he/she is not subject of a punishment issued by an effective court verdict or misdemeanour sanction – a ban to perform a profession, a business or a duty.
- has acquired at least 240 ECTS credits or completed a VII degree of education,
- has working experience of at least 7 years in the fields of law, telecommunications and information technology or 5 years working experience in non-governmental organizations in the fields of protection of human rights, security and defense.

Termination of a mandate

Article 49

(1) The mandate of the President and the member of the Council may be terminated due to following reasons:

- upon his/her request,
- if he/she permanently loses capacity to perform the function,
- if he/she is convicted with an effective court verdict for a criminal act to an unconditional sentence of imprisonment in duration of at least six months.

(2) Grounds to terminate the mandate of the President and of the member of the Council shall be the following:

- unprofessional and reckless work
- violation of the security of classified information;
- abuse of personal data;
- failure to act in accordance with the provisions of the Law on Prevention of corruption.

Reports of the Council
Article 50

(1) The Council shall submit an annual report before the Assembly of the Republic of North Macedonia for the work of the Council for the previous calendar year by the end of February of the current year, at the latest.

(2) The report referred to in paragraph (1) of the present Article shall be considered at a session of the Assembly of the Republic of North Macedonia.

(3) When necessary and upon request of the Assembly of the Republic of North Macedonia, the Council shall submit additional reports.

(4) The public shall be informed accordingly about the report referred to in paragraph 1 of the present Article.

Acting of the Council
Article 51

(1) The Council acts upon its own initiative or upon a complaint filed by a citizen.

(2) The Council, upon a complaint filed by a citizen shall be obliged to:

- immediately submit a request to the Committee referred to in Article 38 of the present Law in order to perform supervision as stipulated in Article 40 of the present Law with the purpose of ascertaining whether the telephone number provided by the citizen is being or has been unlawfully intercepted in the last three months, and
- perform supervision in OTA and authorised bodies

(3) The Committee on the basis of the performed supervision, referred to in paragraph 2, indent 1 of the present Article shall notify the Council within 15 days from the submission of the request.

(4) For the purpose of preserving confidentiality of the interception of communication measures, the notification referred to in paragraph (3) of the present Article shall only state whether in the specific case:

a) an infringement has been found, or

b) no infringement has been found.

(5) The supervision referred to in paragraph 2, indent 2 of the present Article shall be performed by the Council with previous announcement in OTA and in the authorized bodies, in order to compare the data from the anonymized copies of the orders for the needs of supervision and control for the period of the last three months.

(6) The Council, pursuant the notification referred to in paragraph (3) of the present Article and the performed supervision referred to in paragraph (5) of the present Article, shall immediately inform the citizen referred to in paragraph (2) of the present Article, and in the event that an abuse has been ascertained, the Council shall immediately inform the competent Public Prosecutor.

(7) When the Council acts upon its own initiative, the supervision shall be performed in accordance with paragraph (5) of the present Article.

(8) For the performed supervision, referred to in paragraph (7) of the present Article, the Council shall inform the Public.

Rules of procedure of the Council

Article 52

The Council shall adopt Rules of Procedure for its work regulating issues on the procedure and the manner of work of the Council.

Conditions for Work of the Council

Article 53

(1) The work premises of the Council shall be provided by the Assembly of the Republic of North Macedonia.

(2) The funds for the work of the Council shall be provided from the Budget of the Republic of North Macedonia.

1.3. Supervision by the Personal Data Protection Directorate

Personal Data Protection Directorate

Article 54

The Personal Data Protection Directorate shall perform supervision over the legitimacy of undertaken activities during personal data procession, as well as over the application of measures for their protection as specified by law and the regulations adopted on the basis of that law.

1.4. Supervision by the Classified Information Security Directorate

Classified Information Security Directorate

Article 55

The Classified Information Security Directorate shall perform supervision over legitimacy of handling classified information as specified by law and regulations adopted on the basis of that law.

1.5 Supervision by the Ombudsman of the Republic of North Macedonia

Ombudsman of the Republic of North Macedonia

Article 56

The People's Ombudsman of the Republic of North Macedonia shall perform supervision over legitimacy of undertaken activities in implementation of measures for interception of communications from the aspect of protection of human rights and freedoms.

LAW ON CLASSIFIED INFORMATION

Official Gazette of the Republic of North Macedonia no. 275/2019

Article 52

At the request of the Directorate for Security of Classified Information, operational checks for the existence of security barriers to access and handling of classified information are performed by:

- The National Security Agency for all natural and legal persons, except for the persons defined in line 2 of this paragraph and
- the competent services of the Ministry of Defense for all employees of the Ministry of Defense and the Army of the Republic of North Macedonia.

Article 53

The procedure for conducting a security check lasts up to:

- four months for the first-degree security check for individuals,
- six months for the second-degree security check for individuals,
- six months for the third-degree security check for individuals and
- six months for security check for a legal entity.

As an exception to paragraph 1 of this Article, the third-degree security clearance procedure for the persons appointed in the supervisory bodies that supervise the implementation of the measures for interception of communications, as well as for the hired accredited national and international technical experts from those bodies, in accordance with The Law on Interception of Communications lasts one month from the day of submitting the request.

As an exception to paragraph 1 of this Article, the second-degree security clearance procedure for persons before employment in the Operational-Technical Agency, in accordance with the Law on Operational-Technical Agency, lasts one month from the day of submitting the request.

Article 57

The Director of the Directorate may decide to reject the request for issuance of a security certificate for individuals and legal entities if the conditions of this law are not met.

The decision referred to in paragraph 1 of this Article does not explain the reasons for rejecting the request for issuance of a security certificate.

Against the decision referred to in paragraph 1 of this Article, the person whose request has been rejected may file an appeal to the State Commission for deciding in administrative procedure and employment procedure in the second instance regarding the procedure for issuing the security certificate.

Article 58

The appeal referred to in Article 56 paragraph 3 and Article 57 paragraph 3 of this Law shall be submitted within 15 days from the day of receiving the decision, to the State Commission for deciding in administrative procedure and employment procedure in the second instance.

The decision on the appeal referred to in paragraph 1 of this Article, adopted by the State Commission for deciding in administrative procedure and employment procedure in the second instance, is final.

Article 65

The state and local government bodies established in accordance with the Constitution of the Republic of North Macedonia and by law, legal entities established by the Republic or the municipalities, the City of Skopje and the municipalities in the City of Skopje and other legal entities are obliged to create conditions necessary for the protection of classified information and take measures to eliminate adverse consequences if classified information is disclosed.

For efficient and coordinated execution of the rights and obligations related to the classified information, in the subjects from paragraph 1 of this article, an officer for the security of classified information is appointed.

RULES OF PROCEDURE OF THE ASSEMBLY OF THE REPUBLIC OF NORTH MACEDONIA

III. RIGHTS AND OBLIGATIONS OF THE MEMBERS OF THE ASSEMBLY

5. Interpellation

Art. 45

(1) an interpellation may be raised by at least five (5) members of the assembly for the work of any public official, the government and each member of the government separately, as well as for issues related to the work of the state bodies.

(2) the interpellation motion shall be submitted in writing, signed by all the members of the assembly submitting it and it shall contain explanatory notes.

(3) the interpellation motion shall be submitted to the president of the assembly, who forwards it to the person it is addressed to and to the members of the assembly

Art. 46

The person who is the subject of the interpellation shall be entitled to submit a written answer to the president of the assembly within 15 days from the day of receiving the interpellation.

Art. 47

(1) the interpellation motion shall be put on the agenda on the first consecutive session of the assembly, after the expiration of fifteen days from the submission of the answer to the members of the assembly.

(2) if the answer is not submitted within the time frame determined in article 46 of these rules of procedure, the interpellation motion shall be put on the agenda on the first consecutive assembly session.

Art. 48

(1) one of the members of the assembly who have submitted the interpellation motion shall be entitled to give an explanation of the interpellation, in duration of 20 minutes.

(2) the person that is the subject of the interpellation motion shall be invited at the session and shall be entitled to explain his/her answer or give a verbal answer to the interpellation, in duration of 20 minutes.

Art. 49

(1) the debate on the interpellation shall last no more than one (1) working day, until the exhaustion of the applicants for the floor, and it shall be decided at latest at 24:00.

(2) the members of the assembly shall inform the president of the assembly of their

participation in the debate on the interpellation motion 24 hours prior to holding of the session.

(3) the order of members of the assembly by parliamentary groups and members who are not organised in parliamentary groups and who shall participate in the debate, shall be determined by the president of the assembly in agreement with coordinators of parliamentary groups, in such a manner 2 v.s. 1, benefiting the MPs belonging to the opposition political groups and the MPs of the opposition that are not organized in political group

(4) if the assembly endorses the interpellation, it adopts a conclusion containing the position of the assembly in reference to the contents of the interpellation.

Art. 50

Members of the assembly having submitted the interpellation motion may withdraw it only prior to the beginning of the debate.

Art. 51

The debate on the interpellation shall be interrupted if:

- a question of confidence in the government is raised;
- the government resigns;
- the president of the government proposes to dismiss the government member who is the subject of the interpellation, and
- the public official resigns.

XII. RELATIONS WITH THE GOVERNMENT

Art. 212

Trustees appointed by the government shall attend the sessions of working bodies and shall inform and give explanations on the items in the agenda.

Art. 213

The Assembly shall exercise political monitoring and supervision of the Government in a manner and procedure determined by the constitution and these rules of procedure.

DEFENSE AND SECURITY COMMITTEE

The Committee has a chairperson, twelve members and their deputies.

The Committee considers issues regarding the:

- protection of the order established by the Constitution;
- exercising oversight in the field of defense and security;
- defense of the Republic and civil protection;
- cooperation with collective security and defense systems to which the Republic has acceded;

- the integration of the Republic in the Euro-Atlantic organizations and the relations of the Republic with those organizations;
- protection of the life, personal safety and property of the citizens guaranteed by the Constitution;
- production, trade, procurement, possession and carrying of weapons, parts for weapons and ammunition;
- protecting persons and objects;
- citizenship;
- maintaining public order and peace;
- public gatherings and public events;
- safety of road, air, rail and lake traffic;
- protection against natural disasters and epidemics;
- check-in and check-out at the place of residence and stay;
- crossing the state borders and movement and stay in the border zone;
- movement and residence of foreigners;
- determining and resolving border incidents and other violations at state borders,
- establishing international cooperation on defense and security issues; and
- other defense and security issues.

COMMITTEE FOR SUPERVISING THE WORK OF THE NATIONAL SECURITY AGENCY AND THE INTELLIGENCE AGENCY

The Committee has a Chairperson, eight members and their deputies.

The Committee considers issues regarding the:

- respecting of the freedoms and rights of the citizens, companies and other legal entities, stipulated by Constitution and Law, by the National Security Agency and the Intelligence Agency;
- respecting the Law in exercising the authority of the National Security Agency and the Intelligence Agency in terms of encroaching their authority, unauthorized activities, abuse and other adverse trends in its work, contrary to their rights stipulated by law;
- methods and means used by the National Security Agency and the Intelligence Agency in terms of respecting the Law and respect of civil and the rights of other subjects;
- financial, personnel and technical facilities of the National Security Agency and the Intelligence Agency;
- establishment of international cooperation on issues referring to such supervision and
- other issues regarding the National Security Agency and the Intelligence Agency.

COMMITTEE ON OVERSIGHT OF THE IMPLEMENTATION OF THE SPECIAL INVESTIGATION MEASURE INTERCEPTION OF THE COMMUNICATION BY THE MoI, THE FINANCIAL POLICE OFFICE, CUSTOMS ADMINISTRATION AND THE MoD

The Committee has a Chair, 4 members and 4 Deputy Members.

The Committee reviews issues in regard with:

- Oversight of the implementation of the special investigation measure for interception of the communication by the Ministry of Interior, Financial Police Office, Customs Administration and the Ministry of Defence;
- Legal aspect of the application of the special investigation measure for interception of the communication by the Ministry of Interior, Financial Police Office, Customs Administration and the Ministry of Defence from the aspect of their harmonization with the Law on Communication Interception;
- establishment of international cooperation for affairs in regard with this oversight,
- Other affairs in regard with the Ministry of Interior, Financial Police Office, Customs Administration and the Ministry of Defence in regard with the special investigation measure for interception of the communication.

The Committee shall submit a Report to the Assembly of the Republic of North Macedonia two months after the end of the current year, on the oversight of the legal aspect in the enforcement of the special investigation measure for interception of the communication by the Ministry of Interior, Financial Police Office, Customs Administration and the Ministry of Defence.

6.3. ANNEX C: A GENERIC COMMITTEE ANNUAL ACTIVITY PLAN

This is a possible roadmap to activities to be implemented by the committee within a year.

Annual activity plans may help committee, individual members and the staff to organise their agenda, communicate better with overseen institutions and with the public, and plan the engagement of external expertise and other resources. Such a plan could be built up every year, based on the customary practice developed by the committee in the previous year. It can be shared with overseen institutions, the parliament and the public, or not, upon the decision of the committee.

Period	Activities	Follow –up
FIRST PARLIAMENTARY SESSION (FEBRUARY-JULY)	Annual Activity Reports are debated and approved: 1. NSA 2. Intelligence Agency (AR) 3. OTA	Activity reports and debated in the committee with representative of the service Recommendations are formulated in written, and send to the service after the meeting, with timelines for implementation Committee Opinions on the intel activity is submitted/discussed in the plenary
	Committee requests specific reports on issues identified as priorities - specific reporting requirements are drafted by committee staff and sent to the overseen institution	Special reports are received and debated in the committee Recommendations are sent back, with timeline for implementation Press release to sum up the issue, if the topic is not super sensitive.
	Oversight hearings • 2 Proactive – planned in advance, on big policy / reform issues • Reactive– to different issues revealed by media, MPs, independent sources. Public officials invited with 24-48 hours in advance.	Recommendations Report on website Press release
	One joint meeting with other committee(s) holding competencies in intel oversight/ or the Citizens Supervision Council	Joint Opinion on website Plan for joint action
	Legislative activity	Opinion submitted to • other committees • Plenary
	Field Visits/inspections • 2 Planned • 2 Un-planned	

Period	Activities	Follow –up
SECOND PARLIAMENTARY SESSION (SEPTEMBER-DECEMBER)	Annual Report of the Audit Office is debated - Budget execution review for the previous year	Opinion submitted to Plenary Recommendations
	Joint meeting with the Budget Committee	Joint Recommendations
	4 Oversight Field Visits	Press conference/press release Committee Opinion delivered to institution visited (submitted as well to the plenary?)
	4 Hearings– on the implementation of committee recommendations from the beginning of the year	Press release New recommendations are issued Committee Opinion on website (submitted to plenary?)
	Budget proposal for next year is reviewed Joint meeting with the Budget Committee	Opinion submitted to Plenary
	Legislative activity	Opinion submitted to Plenary

6.4. ANNEX D: OVERVIEW OF ISSUES IN ANNUAL ACTIVITY REPORTS

Issues /topics covered in public activity reports	Frequency	Quantitative Indicators	Interpretation/follow up questions & examples from other countries reports
Risks and threats to national security	Yearly	Only *qualitative* indicators	-
Priorities in the work of the service	Yearly	Only *qualitative* indicators	-
Communications interceptions for national security	Yearly	No. of warrants No. of warrant requests rejected by judge No. of indictments & convictions following previous years interceptions No of breaches & mistakes in implementing interceptions procedures	Information on warrants can be also detailed further on number of • cases for which interceptions were requested • people who were intercepted How were procedures changed/tighten as a consequence, to prevent further breaches? *In 2014, Romanian SRI Implemented 44.759 interceptions of communications, of whom 2'762 were related to national security (SRI 2014 Yearly Activity Report, p.31)* *In New Zealand during the reporting period 2016/17 25 domestic and 12 foreign intelligence warrants were issued, while 25 domestic and 10 foreign intelligence warrants were still in force from the previous reporting period. The average days an intelligence warrant was in force was for domestic warrants 172 days and for foreign warrants 153 days. (New Zealand Security Intelligence Service Annual Report 2017, p.34).*

Issues /topics covered in public activity reports	Frequency	Quantitative Indicators	Interpretation/follow up questions & examples from other countries reports
Communications interceptions for criminal investigations (for the Public prosecutor)	Quarterly	Number of warrants executed	*In 2014 Romanian SRI implemented 44'759 interceptions of communications, of whom 42'263 were interception warrants for the Public Prosecutor, on criminal investigations (15% increase to previous year) (SRI 2014 Yearly Activity Report, p.31)*
Intelligence reports produced for different beneficiaries	Yearly	Number of reports Number of beneficiaries	What feedback do the beneficiaries send back? Are the reports used in political decision making? How is the service adapting its intel products following the feedback? *Croatian SOA has submitted in 2014 approx. 8700 reports to its beneficiaries, out of them 290 analytical reports to the President and the Government. (SOA Public Report 2015, p.24) In 2017, the SOA delivered 450 analytical reports to state leadership, which was an increase of 40% to the previous year (SOA Public Report 2017, p.5)* *Romanian SRI has submitted in 2014 5'373 reports to main beneficiaries (10% less than previous year as result of intelligence integration) and 2'937 reports to local administration. (SRI 2014 Yearly Activity Report, p.16)* *Dutch AIVD has produced in 2016 a total of 457 intelligence reports, 152 official reports and 118 threat products. (AIVD Annual Report 2016, p.9)*
Investigation of hints/tip-offs	Yearly	Leads received and Investigated	*Australian ASIO received in 2016-17 over 12 000 leads and resolved or investigated approximately 15 000 lead referrals. (ASIO Annual Report 2016-17, p. 48)* *In 2016, Dutch AIVD dealt with almost 5'400 terrorism related tip-offs, which prompted 238 further investigations (AIVD Annual Report 2016, p.4)*

Issues /topics covered in public activity reports	Frequency	Quantitative Indicators	Interpretation/follow up questions & examples from other countries reports
Organisation and management of the service	Yearly		The organisational chart and functions of different organisational units are often public. Precise numbers of employees are usually classified. Percentage such as gender, education or age is in some cases indicated.
Internal control and oversight	Yearly	Number of complaints Number of disciplinary procedures initiated	*Romanian SRI - 31.397 complaints received in 2016, 20'567 solved favourably. (Relațiile SRI cu cetațenii in anul 2016)* *Croatian SOA - 9 disciplinary procedures in 2014 for violation of official duties (SOA Public Report 2015, p.39)* *In 2016 24 complaints about the Dutch AIVD were made to the Minister of Interior, and 15 to the National Ombudsman (AIVD Annual Report 2016, p.12)*
Public accountability – requests based on Freedom of Information Act		No of. requests received / responded	*Romanian SRI has received 85 Freedom of Information requests in 2016 (positively responded 32, rejected 53) (Annual Report on access to information of public interest 2016)*
Budget – overall amount. Personnel expenses, current expenditures, development and modernisation.	Yearly	Compare with lump amounts from previous years.	Lump amounts are published in public annual activity reports. However, committee should have access to more detailed information on budget execution.

Issues /topics covered in public activity reports	Frequency	Quantitative Indicators	Interpretation/follow up questions & examples from other countries reports
Security Vetting	Yearly	Number of people vetted	Vetting includes access to personal data, therefore it needs to be carried out following transparent procedures; allow for appeal/contestation mechanisms. *In 2016-17, Australian ASIO finalised 27 182 security assessments in relation to Australian Government personnel, and others who require access to nationally classified, sensitive and privileged government information and area, and 14'358 visa security assessments. (ASIO Annual Report 2016-17, p. 54)* *In 2016, Dutch AIVD and mandated organisations (National Police Service, Royal Military Constabulary) completed over 35 000 security screenings (8 000 by AIVD itself). (AIVD Annual Report 2016, p.12)* *In 2014 Croatian SOA carried out 5933 security vetting procedures, (SOA Public Report 2015, p.24) and completed in 2016 security screening of 73'551 individuals (SOA Public Report 2017, p.25)*
Cooperation with other national institutions	Yearly	Sharing of reports amongst national partner agencies	*In 2016-17, Australian ASIO published a total of 1433 intelligence reports for national partner agencies. Reporting was distributed to more than 130 federal, state and territory government organisations. (ASIO Annual Report 2016-17, p. 36)*

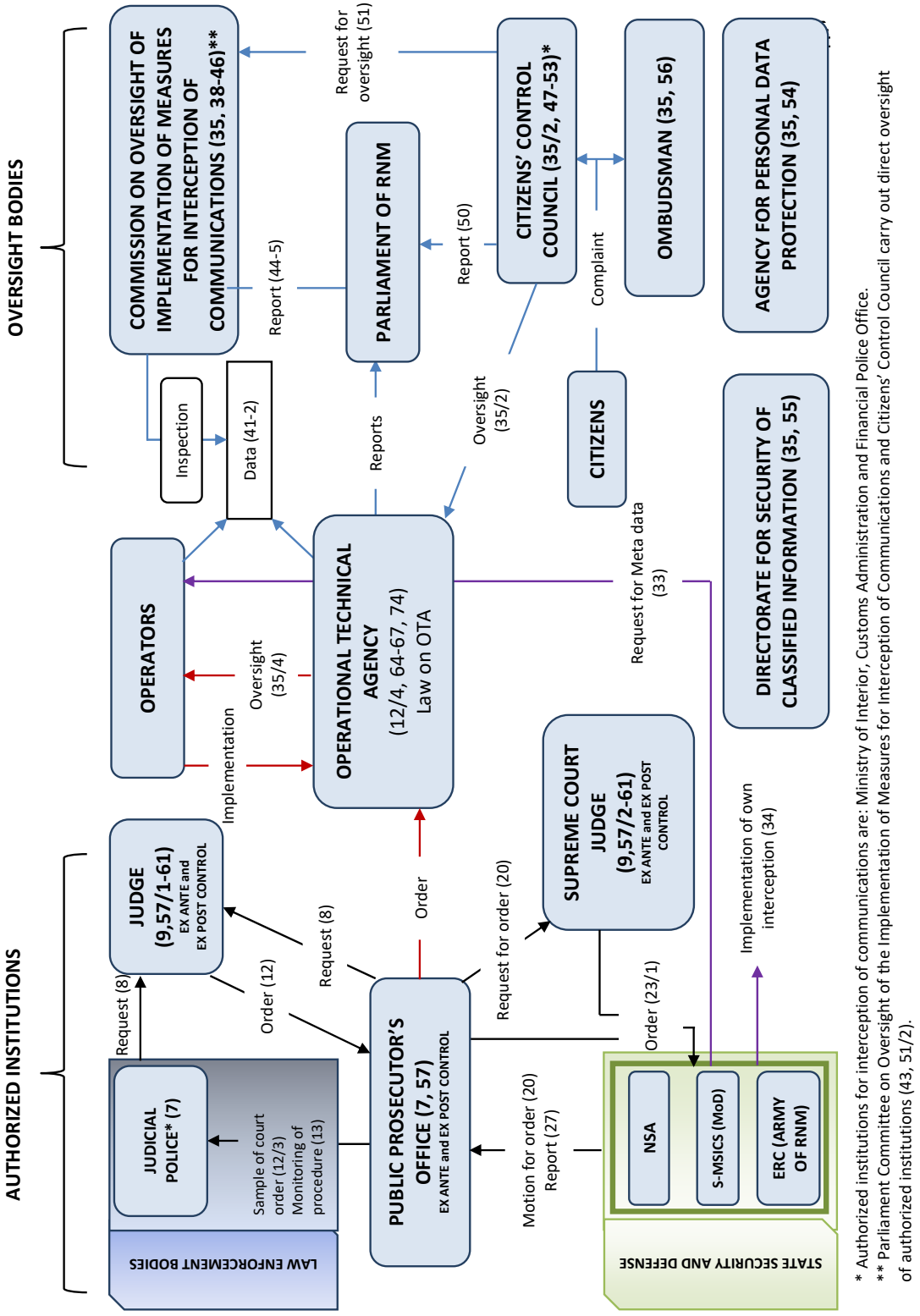
Issues /topics covered in public activity reports	Frequency	Quantitative Indicators	Interpretation/follow up questions & examples from other countries reports
Training / informing of national institutions	Yearly	Delivering of briefings	*Australian ASIO (2016-17) delivered 76 briefings to Australian Government and industry partners on indicators of mobilisation to violence, to build a collective understanding of terrorist behaviour. (ASIO Annual Report 2016-17, p. 51)*
Cooperation with foreign partners	Yearly	Number of countries / or services they have cooperation agreements and exchange of information	*Australian ASIO (2016-17) was authorised by the Attorney-General to cooperate with over 350 agencies in 130 countries. ASIO shared in that period reporting with over 130 foreign liaison partner agencies in 60 countries, with 643 intelligence reports released to one or more partner agencies. (ASIO Annual Report 2016-17, p. 52)* *Between 2013 and 2016 Croatian SOA increased the amount of security intelligence obtained through intelligence cooperation by factor 5. (SOA Public Report 2015, p.13)*
Physical security	Yearly	Number of sites inspected, reported and certified	*In 2016-17, Australian ASIO has conducted:* *Zone 5 facilities: 80 site inspections / reports, 39 certifications* *Destruction services : 9 site inspections / reports, 8 certifications* *Lead agency gateway facilities: 3 site inspections / reports, 2 certifications* *Courier services: 3 site inspections and reports* *(ASIO Annual Report 2016-17, p. 65)*
Technical surveillance countermeasures	Yearly	-	*Australian ASIO: confidential*

Issues /topics covered in public activity reports	Frequency	Quantitative Indicators	Interpretation/follow up questions & examples from other countries reports
Education	Yearly	*Courses conducted*	*In 2016-17, Australian ASIO has delivered 50 courses on situational awareness, personal security, de-escalation, trauma first aid and hostile environment awareness to a total of 512 participants. (ASIO Annual Report 2016-17, p. 68)*

6.5. ANNEX E: OVERVIEWS OF ACTORS AND PROCESSES

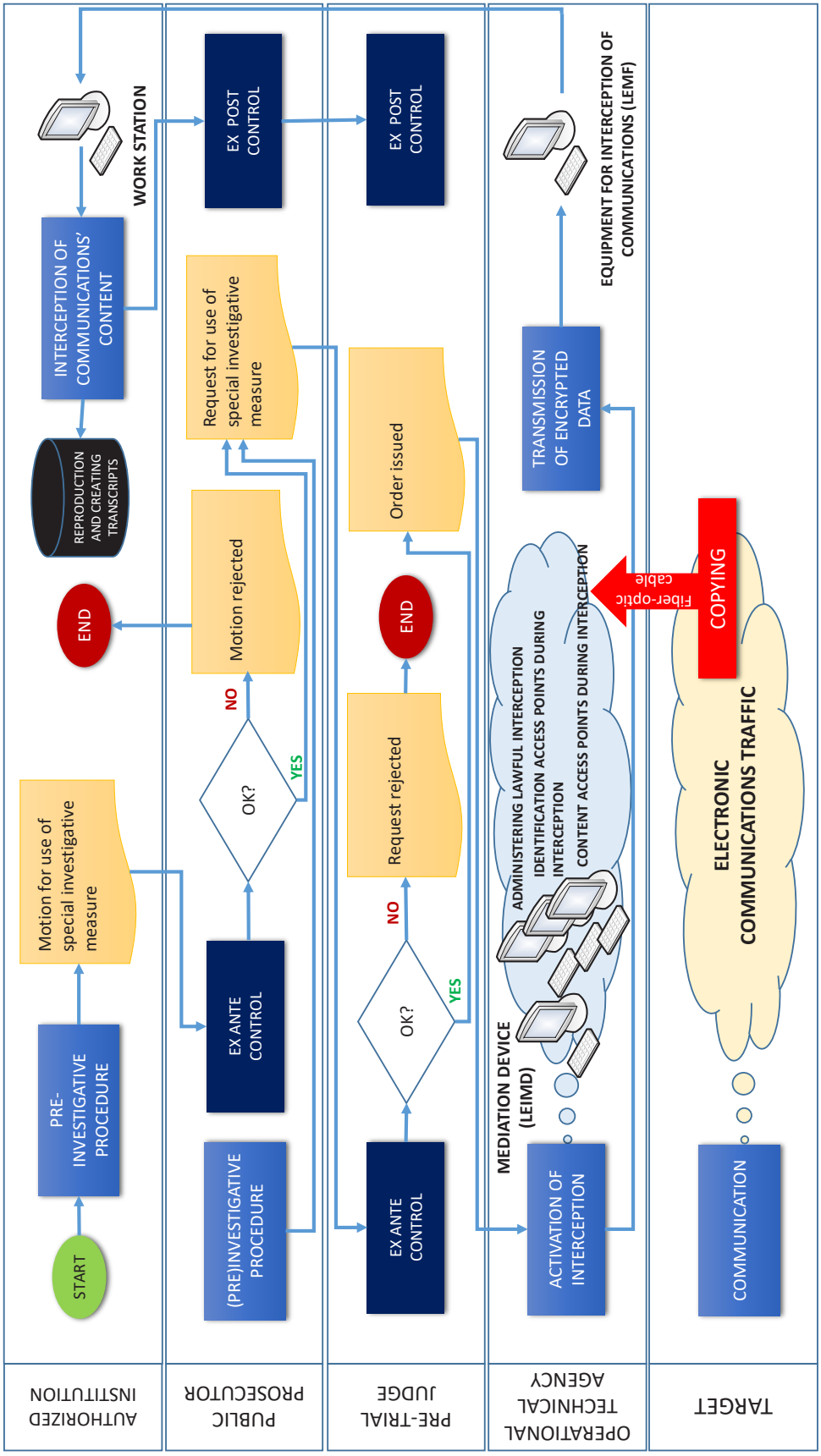
LAW ON INTERCEPTION OF COMMUNICATIONS (I/C) STAKEHOLDER CONNECTIONS

(Numbers in Graph below are referring to Art. in the Law)

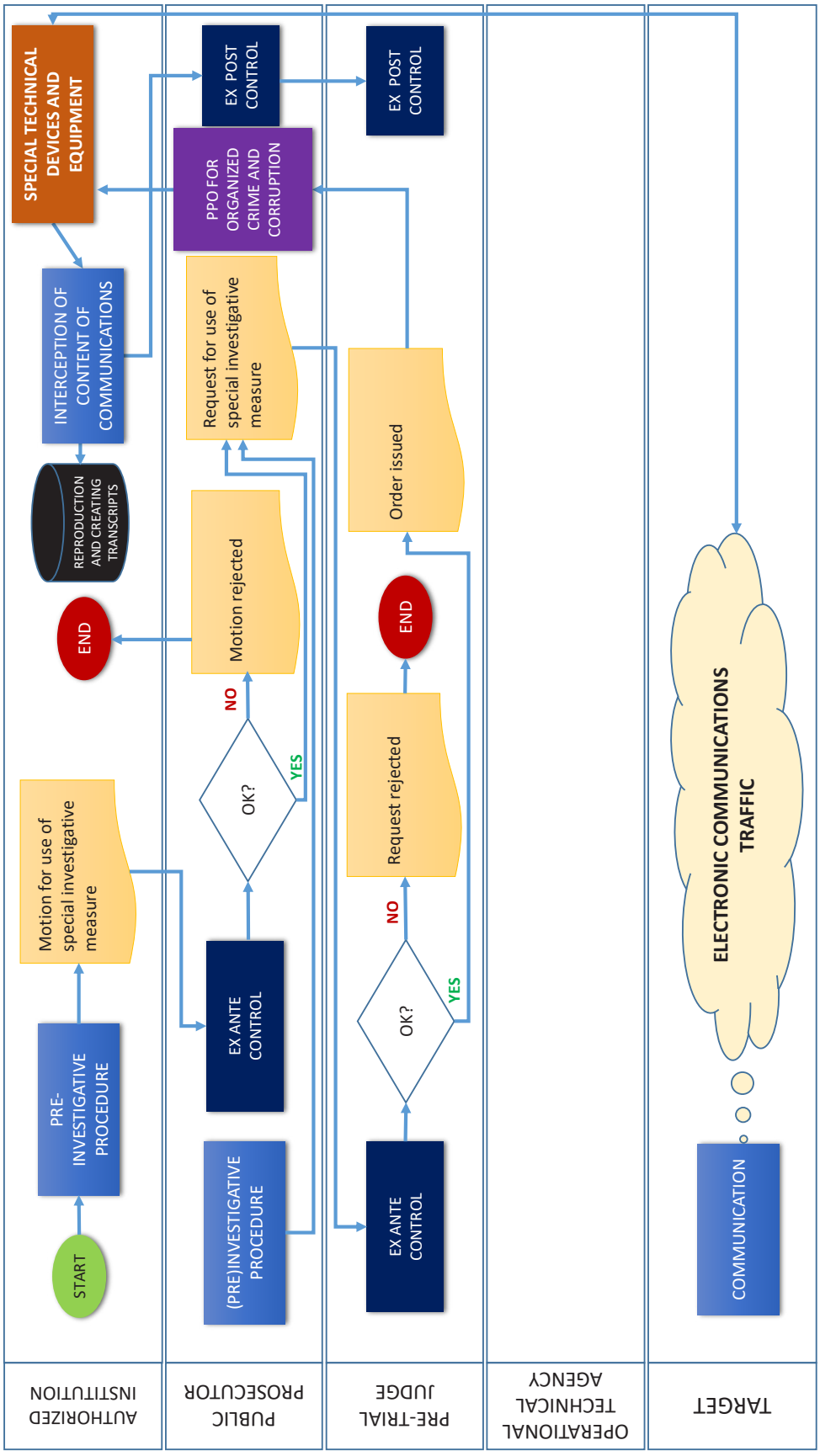


* Authorized institutions for interception of communications are: Ministry of Interior, Customs Administration and Financial Police Office.
** Parliament Committee on Oversight of the Implementation of Measures for Interception of Communications and Citizens' Control Council carry out direct oversight of authorized institutions (43, 51/2).

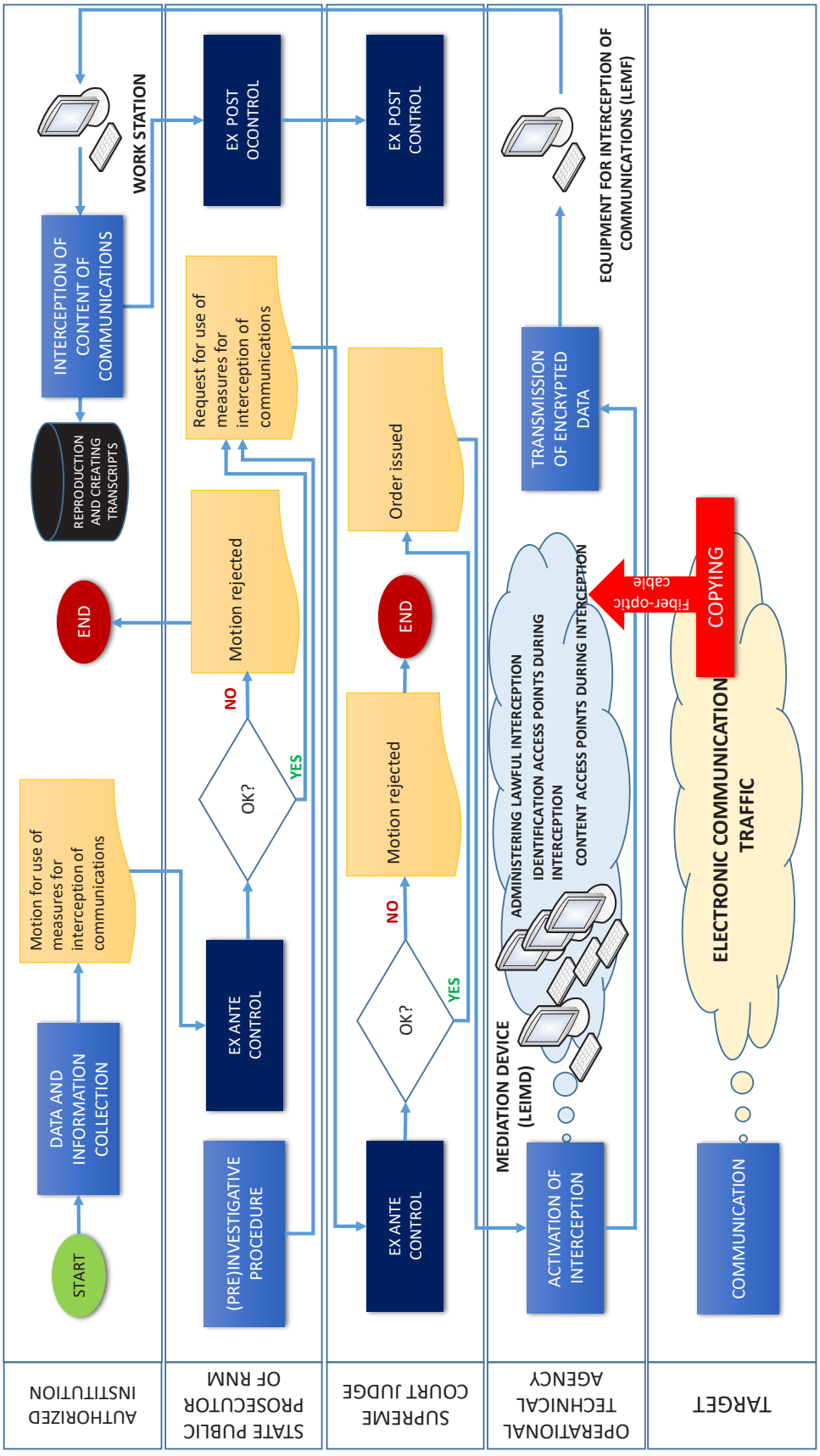
INTERCEPTION OF COMMUNICATIONS IN CRIMINAL INVESTIGATION WITH MEDIATION OF OTA



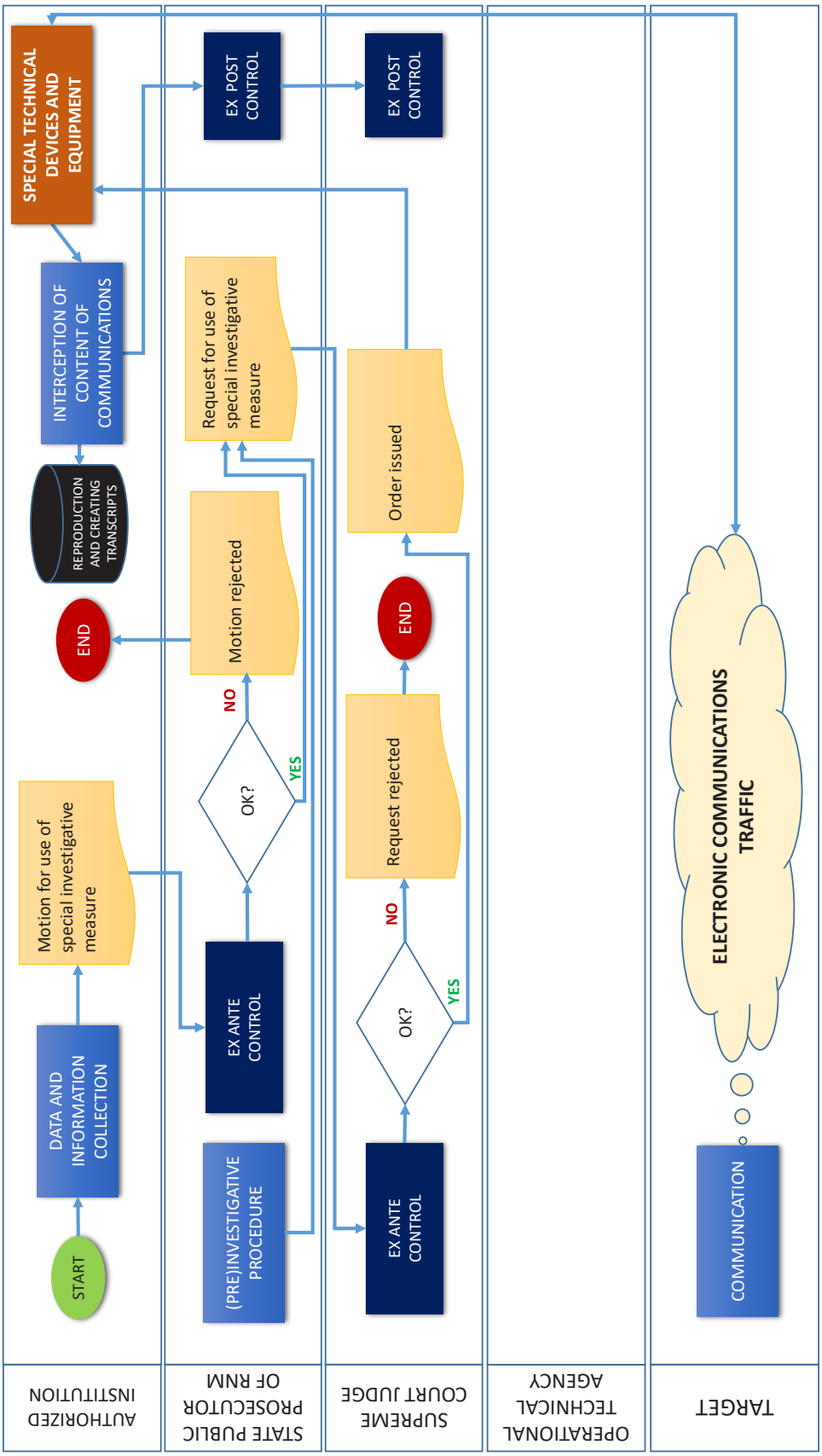
INTERCEPTION OF COMMUNICATIONS IN CRIMINAL INVESTIGATION WITHOUT MEDIATION OF OTA



INTERCEPTION OF COMMUNICATIONS IN INTELLIGENCE AND SECURITY OPERATIONS WITH MEDIATION OF OTA



INTERCEPTION OF COMMUNICATIONS IN INTELLIGENCE AND SECURITY OPERATIONS WITHOUT MEDIATION OF OTA



Technical design:

Marija Dambova Tutkovska

CIP - Каталогизација во публикација

Национална и универзитетска библиотека „Св. Климент Охридски“, Скопје

342.536.078.3:355.45(497.7)(035)

GUIDELINES for Intelligence Oversight : for parliamentary committees in the Assembly of the Republic of North Macedonia [Електронски извор] / [Teodora Fuior ... и др.]. - Текст во PDF формат, содржи 123 стр. ; табели. - Skopje : Centre for Security Sector Governance - Geneva, Skopje branch office DCAF, 2021

Начин на пристапување (URL):

https://dcaf.ch/resources?type=publications. - Наслов преземен од екранот. - Опис на изворот на ден 08.03.2021. - Фусноти кон текстот. - Други автори: Magdalena Lembovska, Julian Richards, Wouter de Ridder, Igor Kuzevski, Ice Ilijevski, Vlado Gjerdovski, Kire Babanoski. - Содржи

и: Annex A, Annex B, Annex C, Annex D, Annex E

ISBN 978-608-66657-0-8

COBISS.MK-ID 53330181