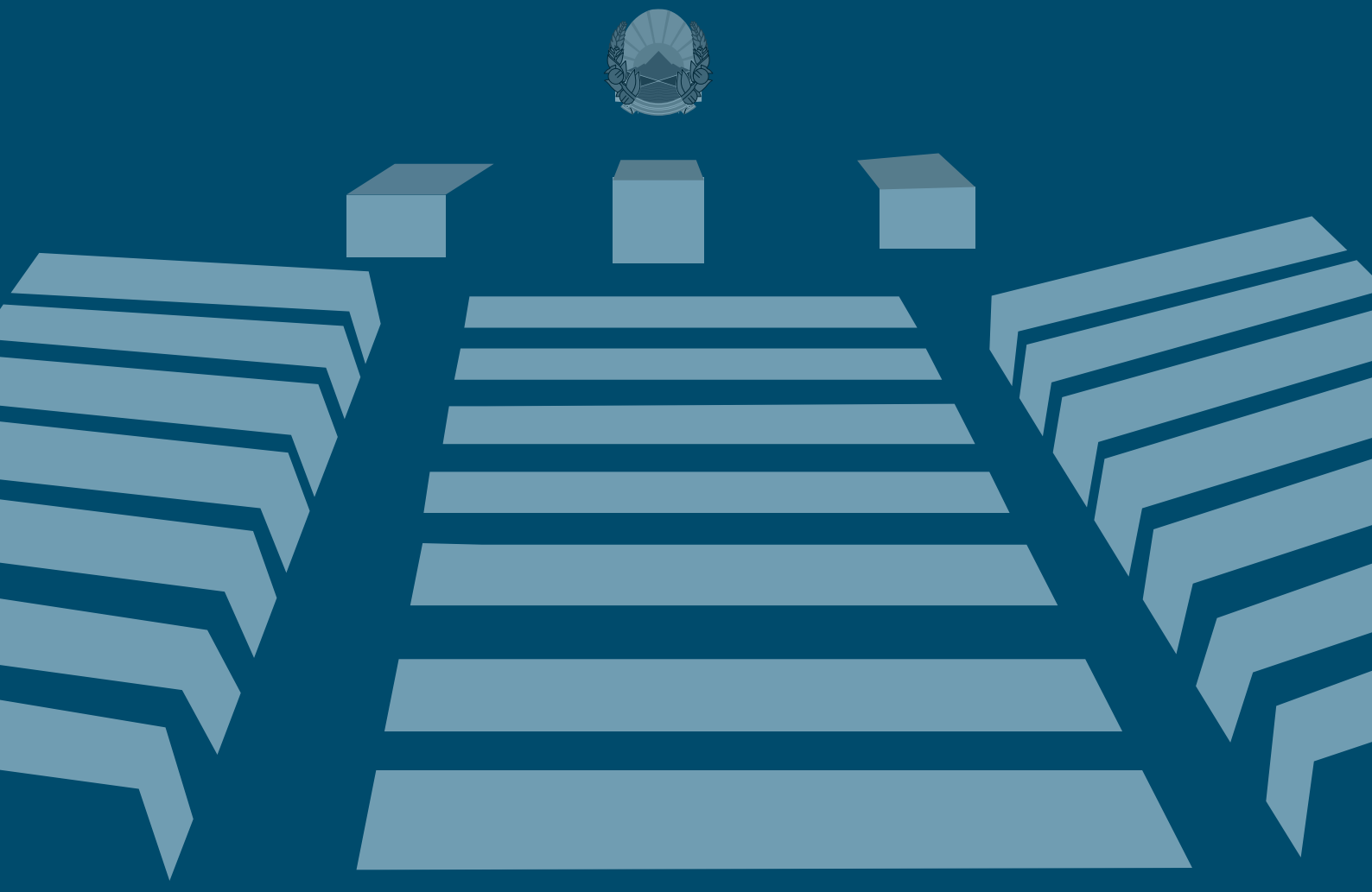
GUIDELINES FOR INTELLIGENCE OVERSIGHT

for parliamentary committees in the Assembly of the Republic of Macedonia



May 2018

DCAF
a centre for security, development and the rule of law

ASSEMBLY OF
THE REPUBLIC OF MACEDONIA

GUIDELINES FOR INTELLIGENCE OVERSIGHT

for parliamentary committees in the Assembly of the Republic of Macedonia

DCAF
a centre for security, development and the rule of law

ASSEMBLY OF THE REPUBLIC OF MACEDONIA

May 2018

Acknowledgements

The completion of these Guidelines for Intelligence Oversight would not have been possible without the valuable contributions and support of a number of individuals.

Thanks are due, first of all, to the members of the **Assembly of the Republic of Macedonia** who contributed to the design and development of these Guidelines from the very beginning. They initiated this project and explained to us the practical challenges faced by their committees in security and intelligence oversight. They took time out of their busy schedules to share with the authors perspectives from which we learned a great deal. We hope the Guidelines answer their expectations and needs, becoming a useful and informative tool for the work of the Assembly.

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

As co-authors of this publication, **Magdalena Lembovska, Professor Julian Richards** and **Wouter de Ridder** invested much individual and collective effort, sustained with patience and professionalism over the course of six months. They brought to the text the valuable and diverse perspectives of a researcher, a former senior intelligence manager and an oversight practitioner.

Peter Gill subjected the text to rigorous scrutiny, providing the external review of the Guidelines. I am very grateful for his expedient advice and sensible remarks.

I would like to thank **Andrej Rupnik**, **Marc Remillard**, **Irena Dzajkovska** and **Vlado Gjerdovski,** my colleagues at DCAF, for their valuable comments and feedback. And finally, very special thanks to **Josip Spec** for his diligent editorial support and astute management of translation and publication activities.

Dr. Teodora Fuior, lead author

Geneva, May 2018

DCAF and the Assembly of the Republic of Macedonia gratefully acknowledge the Foreign & Commonwealth Office and the Ministry of Foreign Affairs of the Netherlands for their financial support of the Intelligence Sector Reform Programme including the production of this publication.

The content of this publication does not necessarily reflect the position or the opinions of the UK Government.

Kingdom of the Netherlands

Contents

1. INTRODUCTION: WHAT IS INTELLIGENCE OVERSIGHT AND WHY IS IT IMPORTANT?

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. 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.

[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.

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.

2. THE 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 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. Potential shortcomings in strategic planning and in legislation should be carefully considered, so that intelligence governance and accountability is improved.

Terminology

Intelligence and security service – a state organisation that collects, processes, analyses, and disseminates information related to threats to national security. It has a legal mandate to use intrusive methods for information collection. The service can be an independent agency/service or a department in a ministry (such as defence, interior, justice). Variously called: security service, intelligence service, intelligence agency.

Intelligence sector – all intelligence services and ministerial departments with intelligence activity in the country.

Special powers – the authoritative functions intelligence services have to collect information – such as the power to intercept communications, the power to conduct surveillance, the power to make use of secret information, the power to enter houses clandestinely, etc.

Intrusive methods for information collection – information collection measures which very likely infringe on human rights or constitutionally given rights of citizens, particularly the right to privacy. Utilized for collecting evidence in criminal investigations by police and prosecutorial bodies, or for protection of national security by intelligence services.

Special investigative measures/techniques - information collection measures infringing the right to privacy, employed by law enforcement for collecting evidence in criminal investigations. Sometimes synonymously used with *intrusive methods for information collection*.

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

Control - the power to manage and direct an intelligence service, performed by the intelligence service over itself (internal control) and/or by the responsible minister and his staff (executive control). It can encompass internal oversight, but cannot replace external oversight.

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

Accountability - Relational concept, where one actor has the right to hold the other actor to a set of standards, to judge the fulfilment of responsibilities, and to penalize if those responsibilities are not met.

Governance – Exercise of power and authority affecting the provision of any public good, such as health, education or security. It includes formal government decisions but also informal processes, actors and values that shape decisions and their implementation. Security governance refers to all institutions and actors involved in security provision, management and oversight at national and local levels.

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. Parliament's involvement in the debate and often in the approval of strategic planning documents is the starting point for oversight. 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.

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.

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 Macedonia is the **National Concept for Security and Defence**[2]. 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[3]. The latest National Defence Strategy dates from 2010.

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. 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. Responsibilities for drafting, adopting and updating such documents should be clarified by law; parliamentary committees should put pressure on the government to maintain the timelines of this process.

The **Programme of Government** sets out the medium term political framework for future reforms and the basis upon which legislation, yearly budgets and 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 defines the reform of the Directorate for Security and Counterintelligenece (UBK) as a key

[2] Law on Defence, Art. 17

[3] Strategy for the Defence of the Republic, Law on Defence, Art. 18

priority, whose implementation will be guided by Priebe recommendations and European best practice. Moreover, the Government commits to fully support parliamentary oversight over the service[4].

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 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. Legal framework for intelligence services

International human rights standards and the *rule of law*[5] 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. 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 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)*

[4] See page 27 of the document: Programa_Vlada_2017-2020_ENG.pdf

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

2.2.1 Intelligence Agency

The Intelligence Agency (IA, Agencija za razuznavanja) was established by law[6] in 1995 as an independent state institution. The Director of the Agency is appointed and dismissed by the President, while the Government also has important competences regarding its work. The Law stipulates that "*the Agency is responsible for collecting data and information of relevance for security and defence of the Republic of 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.*"[7] The total budget of the IA is publicly available as part of the state budget, without further breakdown among budget lines. In 2018, the overall budget of IA for 2018 is 222 300 000 denars or approximately 3.4 million Euros. The Agency has 254 employees[8] and is organised in six directorates:

- Strategic Intelligence;
- Intelligence on International Terrorism and Transnational Crime;
- Research and Analysis;
- Technical Intelligence and IT support;
- Security;
- Organizational Matters.

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.[9]
- Parliament has no competences regarding the appointment of the Director.
- 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, 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.

[6] Official Gazette of the Republic of Macedonia no.19/95

[7] Law on the IA: Art. 2

[8] Budget of the Republic of Macedonia for 2018

[9] 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 chanllenging. IA is also not within the oversight structure of the 2018 Law on Interception of Communications.

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.

2.2.2 Directorate for Security and Counterintelligence (UBK)

The Directorate for Security and Counterintelligence (UBK - Uprava za bezbednost i kontrarazuznavanje) is an integral part of the Ministry of Interior (MoI). The work of UBK is not regulated by a statutory law, but through the Law on Internal Affairs[10] which is deficient in terms of establishing clarity of mandate, competences and responsibility. The Director of UBK is appointed and dismissed by the Government, upon a proposal from the Minister of Interior. According to Article 23 of the Law, UBK is responsible for:

- Counterintelligence activity;
- Countering terrorism and protection from terrorism;
- Protection from other activities aimed at endangering or forcibly demolishing the democratic institutions determined by the Constitution;
- Serious forms of organized crime originating from or aimed at the democratic institutions and which could lead to their endangerment or influence on the security of the state.

UBK collects information using open sources, secret collaborators[11], and special measures and procedures for intrusive data collection[12]. Some UBK employees[13] have police powers including arrest and detention. [14] This is not a common practice for European intelligence services, as in a majority of countries they are limited to information gathering, analysis and interpretation, while arrest and detention remain the privilege of police. The combination of police and intelligence special powers makes UBK a powerful institution whose sound oversight and control is of utmost importance.

[10] Law on internal affairs, Official Gazzete of the Republic of Macedonia no.42/14, amended OG 116/2014, 33/15, 33/15, 5/16, 120/16,127/16 and 190/16, Art. 22-31

[11] Law on Internal Affairs, Art. 26

[12] Ibid. Art 30

[13] According to the Law on Internal Affairs, Art. 37, with the Act of Systematization the Minister establishes the workplaces where UBK employees with status of authorized persons for security and counterintelligence have police authorizations and they shall implement police authorizations in accordance with the Law on Police

[14] Ibid. Art 37. Police authorizations are regulated by the Law on Police.

What international standards apply to arrest and detention by intelligence services?

Rationale: The law must prohibit the arrest and detention of individuals for the sole purpose of collecting information; under special circumstances, intelligence services may arrest and detain individuals who have committed a crime against national security or present an imminent threat to national security.

Treatment of detainees: Intelligence services must respect the human rights of the individual they arrested and detained. They must ensure access to a lawyer, contact to family and adequate living conditions while in detention. They must refrain from any forms of mistreatment of detainees. Intelligence services do not have their own detention facilities, but share the facilities used by law enforcement.

Oversight: The courts must review the legality of all detentions, preventing individuals from being detained arbitrarily. In addition, parliamentary bodies, ombuds-institutions and other human rights monitoring bodies conduct inspections of detention facilities (sometimes unannounced).

Source: UN Principles on Detention, International Covenant on Civil and Political Rights, Convention Against Torture.

The internal organizational structure of UBK is based on a territorial principle.[15] However, unlike the IA, the organizational structure of the UBK is not publicly available. The official organigram of the Ministry of Interior[16] does not give any indication about UBK being its integral part. Moreover, the budget of this agency is not publicly available, as it is part of the overall MoI's budget. Also, the number of employees within UBK is not publicly available. The opacity around UBK illustrates the limitations resulting from the absence of a statutory law to define the role, organisation and functioning of an intelligence service. Pursuing the accountability of a service in these circumstances is a difficult task for overseers.

The 2018 Law on Interception of Communications makes the necessary distinction between interception of communications as a special investigative measure (for the purpose of criminal procedure) and interception of communication for the purpose of security and defence (mainly used for prevention and identification of possible threats). The latter is especially sensitive and more secretive because the collected information is not used as evidence in a criminal investigation, therefore the implementation of these measures cannot be sanctioned post-facto by the court.

2.2.3 Military Service for Security and Intelligence (MSSI)

This service (VSBiR – Voena sluzba za bezbednost i razuznavanje) is situated within the Ministry of Defence (MoD) and the Army of the Republic of Macedonia (ARM), but the Law of Defence does not refer to it as a separate organizational unit. Nevertheless, the law defines intelligence and counterintelligence activities for the purpose of defence[17], including:

- 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.

MSSI is composed of one unit within the MoD, the Sector-Service for Military Security and Intelligence and three sections within the ARM units: J-2, S-2, A-2. How MSSI conducts its work is regulated by by-laws derived from the Article 136 of the Law on Defence. The sections in the ARM are double hatted: by command functions under the General Staff of ARM; and by professional functions under the Head of Sector-Service for Military Security and Intelligence.

15 Ibid. Art 22, paragraph 2

16 http://www.mvr.gov.mk/Upload/Editor_Upload/publikacii%20pdf/Organogram%20na%20MVR%20(Celosen)%20-%2014_10_2015-1.pdf

17 Law on Defence, Official Gazette of the Republic of Macedonia 42/01, amended O.G. 5/03, 58/06, 110/08, 151/11, 2015/15, Decision of the Constitutional Court no. 37/2002 (O.G. no 73/2002) and Decision of the Constitutional Court no.37/2002 and 155/2001 (O.G. 78/2002)Chapter XI, Articles 133 - 141

The Sector-Service for Military Security and Intelligence has nine units, including: Unit for planning and general matters, Support unit, Unit for CCIRM[18], Intelligence Unit 1, Intelligence Unit 2, Counterintelligence Unit, Unit for Security, Unit for Physical Security and Unit for Analytics.[19] There is no publicly available information on the 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. Authorized persons from the MSSI have the right to collect data, information and notification[20].

The Centre for Electronic Surveillance (CEI)[21] of the ARM is also granted powers for interception of communications[22], but only in certain radio wave frequencies (High Frequency- HF, Very High Frequency-VHF and Ultra High Frequency UHF) which are specific to defence needs. Hierarchically CEI is not part of MSSI's structure, but is an Army unit subordinated directly to the General Staff. MSSI coordinate with CEI, for professional purposes, through the J-2 Section in the General-Staff.

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;

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.

2.2.4 Operational-Technical Agency (OTA)

The legislative reform of the system for interception of communications adopted in April 2018, established an Operational-Technical Agency (OTA) as a standalone, independent state body. OTA is supposed to have a technical role, facilitating the connection between the authorized bodies[23] and the service providers, on the basis of a court order (Art.2 of OTA Law). Requests for an interception 'order' must be successively approved by the public prosecutor, by the judge, and then passed to the OTA who supervises telecom operators and makes the intercepted information available to the agencies[24]. OTA does not have capabilities to access the content of intercepted communications.

The big step forward in the establishment of OTA is the fact that the technical capability to engage in surveillance is removed from the agency responsible for collecting and analysing intelligence. The UBK is to have no direct access to telecommunications in the new system. This institutional arrangement prevents the concentration of power in one institution, facilitating accountability. 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.

18 Collection Coordination Intelligence Requirements Management (CCIRM)

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

20 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.

21 Centar za Elektronsko Izviduvanje (CEI)

22 Art. 4, Point 7 of Law on interception of communication , Official Gazette of the Republic of Macedonia 71/18

23 In Macedonia there are currently eight bodies mandated to use intrusive methods for information collection, subjected to parliamentary oversight: AR, UBK, the criminal investigation units from Police, Financial Police, Customs, MSSI, ARM/CER, OTA

24 There are two important exceptions to this general oversight process: first UBK, MSSI (Defence) and CER (Army) can ask operators *directly* for metadata (Art. 33 of the Law on Communications Interception) and can also conduct their own interception without reference to court or OTA (Art. 34).

OTA is also subject to oversight by Parliament and other oversight bodies. Overseers will need to ensure OTA remains strictly technical and free from external influence and pressure. The recruitment, vetting and oversight of OTA officials will need to be robust in order to avoid a potential continuation of past abusive practices and mentalities. Attention should be given to the development of by-laws, regulations, professional standards, codes of conduct and personnel training. The oversight of communications interception should give particular attention to a number of legal provisions whose implementation may raise challenges for accountability:

- special technical devices and equipment allowing communications interception (such as IMSI catcher, Wi-If interception etc.) will be kept by the public prosecutor; the use of this equipment should be monitored by overseers and eventually further regulated (LIC Art.17)
- the law (LIC, Art.18) refers jointly to different intrusive methods that should be regulated separately, as the level of intrusion is different, and some are aimed to enable the other (such entering to the private premises to plant audio and video capturing equipment).
- There are three important exceptions to the general oversight process: first UBK, MSSI (Defence) and CER (Army) can ask operators directly for metadata (LIC Art. 33) and can also conduct their own interception without reference to court or OTA (Art. 34). The IA is not covered by the Law on Interception of Communications at all. This falls short of the current European standards established by the jurisprudence of the ECHR and the ECJ.

2.3. The Macedonian Intelligence Oversight System

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

Who is responsible for keeping the intelligence sector accountable?

1. **Internal control** - directing officials and internal control and audit mechanisms. It relies on standing orders, recruitment, training, co-ordination of staff (including mechanisms for protecting the rights of officers and disciplining individuals).
2. **Executive control** – relevant ministers and executive officials. Based on policies, directives, priorities and responsibility to Parliament.
3. **Parliamentary oversight** – relevant oversight committees. Based on laws, parliamentary procedures, oversight activities, approval and review of the state budget.
4. **Judicial review** – independent judiciary. Includes the authorisation of special intrusive powers, and the judgment of alleged violations of the law.
5. **External oversight** - media and civil society. Based on investigative journalism, independent research, public debate of policy alternatives 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 promote a culture of accountability and professionalism, starting with effective recruitment and training processes; they also coordinate processes for evaluating the performance of the staff. Managers must implement robust selection criteria to ensure they only 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 bodies.

- The directors are appointed for a fixed term of office to protect them from political pressure or changes in government; they can only be removed from office if they breach specific rules.
- Internal inspectors-general assess the lawfulness 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; there is no public record on their involvement with UBK. Unfortunately, none of the by-laws specifically referring to UBK are publicly available.
- The **Ministry of Defence** (MoD) conducts internal control through inspectors-general who check whether the employees' performance is in accordance with the relevant laws.
- The **Law on Intelligence Agency** has no provisions regulating internal control.

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 or/and parliamentary committees before 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.

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 activity relies on the 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.

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. Absence of this feedback might result in inadequate intelligence products.

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 demand information from them. 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 in the work of intelligence 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.

What bodies are responsible for the executive control of intelligence?

- broader ministerial portfolios such as defence, interior or home affairs, justice, for intelligence services organised as departments in a ministry
- prime minister (e.g. in UK)
- president (e.g. in Romania)
- joint authority of a president and prime minister (e.g. in Croatia, Slovenia).
- collective body such as a national security council (e.g. Croatia, Romania, Serbia).

In the Republic of Macedonia, as in all other countries, the executive (including the President of the Republic and the Government) are the main beneficiaries of intelligence work. The 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 counterintelligence service (UBK) and military intelligence (MSSI) operate within their respective ministries and are responsible to the Minister of Interior and Minister of Defence respectively.
- The Government appoints and dismisses the Director of UBK, upon a proposal from the Minister of Interior.
- The IA reports directly to the President of the Republic of Macedonia, who has the right to appoint and dismiss its Director. The Government has strong competences regarding IA as it prescribes IA's methods and means of operation, and is also holding the IA Director to account, but the law does not specify how.[25] 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 the minister. The 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 special challenges when carried over to new democratic governments:

- Information collected under a former regime may be used for blackmail, extortion or political manipulation.
- Seeking justice for past abuses may 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 the media in transition states may be ill-equipped or unwilling to scrutinize intelligence.
- The lack of a legal framework for democratic oversight and control, fragmentation of services and broad mandates of intelligence services make oversight difficult.

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 taken by the services.

[25] Law on IA, Art. 4

What are the typical challenges in the democratic oversight of intelligence?

Secrecy: management, control and oversight of a large governmental bureaucracy is more complicated 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 of these is time consuming and difficult.

Political will: because of the level of secrecy involved in intelligence work, many aspects related with intelligence oversight cannot be publicly discussed therefore are not necessarily useful for winning citizens attention and votes. Therefore, elected representatives may lack incentives to invest their time in intelligence oversight.

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

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 more quickly than the mandates and powers for their oversight and control, leading to gaps in accountability. Technical experts can provide oversight bodies with crucial information, while legislatures need to ensure that legal frameworks keep abreast of such changes.

2.3.3 Parliamentary Oversight

Intelligence oversight is one of the newest[26] 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.

What is the scope of intelligence oversight?

- **Legality** – refers to the conformity with all applicable legal provisions from national primary and secondary law, 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 objectives defined by government policy 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.

[26] National security in general and intelligence in particular, have been perceived as the exclusive area of competency for the executive power, legislative and judiciary bodies deferring from interference. Only in the 90s, after the end of the cold war, parliamentary oversight of intelligence has become a norm and a prerequisite of democracy.

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 specialization and organisational complexity.

1) **Defence and security committees.** In some countries one committee with a wide mandate deals with legislation and oversight for the whole security sector, including intelligence services and ministerial departments with intelligence activity; this approach allows committee members to develop a comprehensive understanding of the security sector, and integrate legislative and oversight processes. This is the case today in countries like Albania, Montenegro and Moldova that have a relatively small security sector; however, a decade or two ago this was the approach of 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) specialized working bodies dealing exclusively with intelligence oversight. They have a narrow and focused oversight mandate, so elected members and staff may make best use of time and resources, develop expertise and engage in sustained oversight activities. Sometime the mandate of these committees involves exclusively oversight; their responsibilities in the legislative process being 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 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 parliament and they report to parliament and/or the executive. Belgium, Croatia, Denmark, Germany, Greece, Norway the Netherlands and Sweden provide 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 defense 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 main two services – the Security and Counter Intelligence Directorate from the Ministry of Interior and the independent Intelligence Agency. A third parliamentary committee has a very precise and specialized oversight mandate, monitoring the implementation of intrusive methods for information collection.

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

The legal authority[27] of oversight bodies is the first precondition for effective intelligence oversight. The legal authority of the three Macedonian parliamentary committees relies (1) on general law provisions regulating parliamentary oversight, and (2) on specific provisions regulating intelligence oversight.

(1) The legal foundation for parliamentary oversight is spelled out in the **Constitution** of the Republic of Macedonia, which says "*Parliament carries out political monitoring and oversight of the Government and other public office holders responsible to the Parliament.*"[28] The **Law on the Parliament** has a separate chapter called "Parliamentary Oversight", which regulates hearings as the main tool for oversight.

The Parliament's **Rules of Procedure** are the most detailed legal document regulating the rights and obligations of the MPs, including the right to information, the use of parliamentary questions and interpellation as tools for oversight, 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

[27] Annex 1 reviews the relevant law extracts giving parliamentary committees the legal authority for intelligence oversight

[28] Constitution of the Republic of Macedonia, Art. 68

MPs can use proactively. For instance, in cases where public officials do not present themselves after being 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 the answer contains classified information.

(2) In addition to these general provisions that concern the parliament as a whole, the oversight of intelligence activities, by dedicated parliamentary committees, is prescribed briefly in several laws.

- Article 11 of the Law on the Intelligence Agency provides that "the director is responsible to enable insight and to provide all the information and data within the scope of work of the Committee".
- Article 42 para 1 of the Law on Internal Affairs states that "On the parliamentary committee request, the Directorate will enable insight and provide the committee with the necessary reports, information and data relevant to its work".
- Both services are obliged to submit an annual report on their work to the Committee. UBK also submits an annual work programme[29].

The mandate of the 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[30], the **intelligence oversight committee** (for UBK and IA) has a strong oversight mandate, covering respect of the law in exercising the authority of the services, respect of human rights, and even methods and means used by the services, and financial, personnel and technical facilities. The services have the obligation to provide the information necessary for the accomplishment of the oversight mandate of the committee.

The Law on Interception of Communications (LIC) adopted in April 2018 clarifies and strengthens the legal authority of parliament in the **oversight of communications interceptions**. The parliamentary committee mandated with this task is defined by the following **features**:

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

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

- While the legality refers to interceptions implemented for criminal investigations (judicial police, Art. 7) and also for security and defence purposes (by UBK and MoD, Art.18), the *efficiency* seems to refer only to interceptions for criminal investigations: the law states that this oversight objective is to be accomplished through the analysis of the report of the Public Prosecutor (Art.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. In the letter of the law, oversight seems primarily concerned with ensuring that investigative measures and processes have been implemented properly but this does not exclude the possibility of overseeing operational activities and their efficiency.

Access to expertise. The law stipulates (Art. 39) that no later than 50 days after its appointment the committee shall hire two experts for permanent technical support; within 6 months, the committee must create a roster of national and international experts to provide support on a case by case basis. The law spells out the obligation of other state agencies to provide expert support at the request of the committee. These are exceptional measures intended to

[29] Law on Intelligence Agency, Art.10; Law on Internal Affairs, Art. 61

[30] Parliamentary Decision no. 08-1396/1 from 31 May 2017

increase committee expertise and enhance its ability to engage in effective oversight. Insufficient expertise in intelligence matters is, in every country, one of the biggest challenges in oversight. LIC provides the committee with several different avenues for solving 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 with *legality* is specified in LIC Art.41-3. The committee will be able to check the number of authorizations issued and what type 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. That means it needs to 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 (Art.37) states that oversight body members will "be in possession of a security certificate with an appropriate degree for access to classified information", and such a certificate will be issued within 30 days. 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, competent (data protection) authorities, and where appropriate, the Assembly and the public. The committee can produce special reports when requested by the Assembly. Committee annual reports are to be made public (Art. 45). The law embraces the good practice of stating clear timescales for reports to be published: the Committee shall lay the annual report before the Assembly by the end of each February at the latest (Art. 45(1)), which is quite an ambitious target.

- The law is slightly unclear on when and how the results of investigations and oversight will be made public. The committee will inform the public, where appropriate and without disclosing specific data (Art. 44). The question of what "appropriate" means here and who decides on it should be clarified in the committee Rules of Procedure.
- Another very ambitious reporting target is set up in Art.51: the Committee will notify the Citizen Supervision 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 available to the committee.

The Law on Interception of Communications refers to only 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 of inspiring the other committees to pursue changes in laws, regulations and practice, in order to attain improved 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 procedure**. 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 Art. 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 the members are aware that intelligence oversight is the responsibility of them all.
- **Adopt statutory laws for all intelligence services/departments**. The legislative package on communications interception adopted in April 2018 should be only the beginning of a comprehensive legislative reform of the intelligence sector and its oversight; similar efforts are underway in many European countries (France, Germany, the Netherlands and UK, for example). The legal mandate of all agencies and departments who can make use of intrusive methods for information collection should be defined more clearly, in statutory law the Intelligence Agency`s functioning is based on a specific law but neither military intelligence or UBK. Ambiguities and overlap should be avoided, in order to create a clear foundation for accountability.

- **Consider adopting special legislation on intelligence oversight**. The inherent challenges of the intelligence oversight process require a strong legal base and clear procedures for the work of oversight bodies. 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 the powers of oversight bodies (Germany, Slovenia, Montenegro and Romania are just a few examples). This brings several advantages: it clarifies the rules of the game in oversight and makes the legal authority for oversight incontestable; it may bring increased visibility, prestige and credibility to the responsible oversight bodies; it provides structural and procedural continuity in parliamentary oversight, from one term to another, 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 exactly that all potential for abuse of power is excluded. 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 respondent parliaments)

- oversee services policy and administration, budget and expenditure
- receive reports from the intelligence services and/or the executive;
- may ask the intelligence services and/ or the executive to provide the committee with information.

Enhanced powers (4 out of 24) – the essential powers are enhanced by:

- the power to receive complaints
- initiate investigations on its own initiative and inspect premises,
- issue recommendations or binding decisions;
- might be involved in the authorisation process of surveillance measures.

EU Agency for Fundamental Rights (FRA), Surveillance by intelligence services, fundamental safeguards and remedies in Europe. Mapping members states legal framework, 2015

2.3.4 Other independent bodies

Citizens Supervision Council

The 2018 Law on Interception of Communications establishes another layer of intelligence oversight, through a civil body mandated to supervise the legality of communications interceptions. This is an important step towards building public trust in the intelligence sector, especially because members of the civil society were subject to illegal wiretapping in the past.

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) who will be appointed by the Parliament from public applications. The Council also reports to the Parliament. Moreover, the work premises of the Council shall be provided by the Parliament, which allows for closer cooperation and communication between the parliamentary committees and the Council.

Another novelty 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. Therefore, it is important that the Parliament develops clear rules and procedures that will regulate the cooperation and communication between the two bodies.

The Council is also authorized to supervise OTA and the authorised bodies upon a complaint from a citizen or upon its own initiative. The law is, however, not very clear on how the Council will perform its "supervisory competence", or to which information it will have access. This is particularly important given that the members of the Council will most likely not be experienced in intelligence activities or in government service. Whether it acts on its own initiative (*proprio motu*) or following a complaint, it seems under Art. 51/5 to be limited to looking at anonymized data in the possession of OTA or the (surveillance) authorizing bodies, and then only "after announcement". The investigatory role of the Council seems therefore to be reliant on the investigative powers of the respective parliamentary committee (see Art. 51/2). The Council is only to determine if an infringement has occurred or not (Article 51/4). If it finds abuse it informs the prosecutor (Art. 51/6) and the public (Art.51/7).

There is a risk of duplication of the work of the Council and the committee, but also of having diverging views and findings on the work 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.

Directorate for Personal Data Protection

Data protection agencies play a fundamental role in safeguarding the right to the protection of personal data. The Macedonian Directorate for Personal Data Protection is one of the most important independent oversight bodies when it comes to intelligence oversight, taking into consideration that intelligence services gather and process large amounts of sensitive private data.

The Directorate is an independent institution managed by a Director, who is appointed and dismissed by the Parliament upon previously published public notice, for a period of 5 years with the right of re-election[31]. The Director is obliged to submit an Annual Report to the Parliament, but also an additional report should such a request come from the Parliament. One of the most important instruments for ensuring the protection of personal data are inspections. Regular inspections are carried out according to an annual programme; however, an emergency inspection may also be conducted after a proposal/initiative by a government authority, legal and natural entity, or in case the inspector believes that there has been a violation of the Law on Personal Data Protection[32].

The 2018 Law on Interception of Communications (Art.54) mandates the Directorate for Personal Data Protection to supervise supervising the legality and legitimacy of activities undertaken during personal data processing, and the measures taken for their protection. The Directorate took tangible, public action to correct the misuse of interceptions, conducting several inspections throughout 2016/2017.

[31] Law on Personal Data Protection, Consolidated version (O.G. 7/2005, amended O.G. 103/2008, 124/2008, 124/2010, 135/2011, 43/2014, 153/2015 and 99/2016). Art. 37

[32] Ibid. Art.44-b

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 authorising, 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, Scheinin, M. (2010)

Ombudsperson

The mandates of these officials vary significantly across Europe and most do not play a significant role in intelligence oversight. Even when laws allow them 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 grants it a clear mandate and strong investigative powers. 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 reports to Parliament annually on his/her work, submitting a publicly available report and presenting it during a plenary session of Parliament attended by representatives of the Government. This could be an opportunity for parliament to engage in more detailed dialogues with the Ombudsperson, trying to exchange lessons learned and develop complementarity of action.

State Audit Office

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.[33] 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[34].

In the performance of its mandate, SAO has access to classified information. 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 (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.

2.3.5 Public Prosecution/Judiciary

Judicial control is one of the most powerful safeguards in the use of intrusive methods; therefore legislation should clearly prescribe principles for the ex-ante judicial authorization of a measure and for ex-post judicial review, during implementation and after the measure has been terminated. These principles (such as legitimacy, proportionality, legality, necessity, subsidiarity or ultima ratio) should be binding on all state authorities involved in the initiation, authorization and implementation of intrusive methods for information collection. Besides the authorisation of these measures the judiciary undertakes a few more actions of relevance for intelligence oversight:

- *Adjudicates* charges of misconduct, criminal activity or access to information in intelligence-related matters. So that secrecy does not lead to impunity, special judicial provisions can ensure that the law is applied even while protecting classified information;
- *Provide access to remedy*, in cases where individuals complain about infringements of their rights by security and intelligence services, and challenge an arrest, interrogation, detention or an interference with their privacy;
- *Conducts judicial review*, which 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) contributing their expertise to parliamentary enquiries or oversight commissions or conducting special inquiries.

Judicial protection, as a general principle in the application of intrusive measures, has been somewhat neglected in the past (not only in Macedonia but in most countries) for even when judicial authorization for surveillance was sought and obtained, this was in practice a formality. The judge did not have, or did not regard himself/herself as having, a responsibility to check if the surveillance was justified on material grounds. Instead, the judge only checked the formalities (e.g. was the offence for which surveillance was sought an offence for which surveillance is permitted). Today, such a limited approach to judicial authorization is contrary to European standards and the situation is improving in the Republic of Macedonia as well.

The judiciary has an important role in proposing, approving and implementing special investigative measures in the Republic of Macedonia. Their role is evident in regard to interception of communications, as described in the new Law on Interception of Communications.

The law provides two control layers in the implementation of interceptions for both criminal investigations and

[33] Law on State Audit, Official Gazette of Republic of Macedonia, Art. 23

[34] SAO conducted an audit in the Intelligence Agency in 2007

national security and defence purposes[35]: the Public Prosecutor and the judge issuing the order for interception of communications[36] provide authorisation for interception of communications. Their control covers the legality of the implementation of the measures and the subjects of their control are the authorized bodies, the telecom operators and OTA. Besides authorising the measures, the legislators also provided strong powers to the judiciary: unannounced inspection of sites, equipment and documentation, direct access to the electronic registry system, control of the use of special technical devices and equipment etc.[37]

The Public Prosecutor of the Republic of Macedonia submits an annual report to the Parliament which 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 with most European states, the main system of control over surveillance in the Republic of Macedonia is the judicial, relying on prosecutors and the courts. The oversight provided by parliamentary committee and citizens' council are intended as a "back-up". If the prosecutors do not act as a filter on surveillance applications, and the courts do not take authorization 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.

What are the differences between parliamentary oversight and judicial supervision?

- Parliamentary oversight is more policy-related, whereas judicial review deals exclusively with narrow legal questions; the judiciary only reacts to legal matters brought to its judgment, it cannot take initiatives on its own;
- Parliamentary oversight is, in theory, unlimited. MPs have the democratic legitimacy to request information and explanations about any aspect of the work of a governmental agency and have the right to inspect premises and check intrusive capacities themselves;
- Judges tend to show more deference to the executive branch in national security and intelligence matters than MPs;
- Although parliaments usually have little authority over operational matters, they have broad powers to determine the mandate and budget of the security services, which gives them important leverage in influencing their conduct.

[35] In many European countries requests for the use of intrusive methods for information collection for national security purposes by intelligence services is submitted directly to the responsible judge, without the filter of a prosecutor.

[36] The judge of the preliminary proceedings is responsible for issuing orders in law enforcement cases (articles 7-9) and the judge of the Supreme Court of the Republic of Macedonia for issuing the order in national security cases (articles 20-21). Law on Interception of Communications.

[37] Ibid. Art. 59-60

3. COMMITTEE OVERSIGHT ABILITY: ENABLING CONDITIONS FOR EFFECTIVE OVERSIGHT

For oversight to be credible it needs to be based on clearly defined **legal authority**, embedded in the Constitution and laws, and meeting the democratic standards that make checks and balances functional, and accountability a fundamental principle of governance. The previous chapter of this Guideline reviewed the legislative framework that gives parliament legal authority to engage in intelligence oversight. Institutions and legal provisions that make 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, expertize, 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[38], 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)
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)

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

3.1. Access to information

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

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

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.

(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[39]. 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 provides 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 mechanismsin 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.

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

A committee`s **access to information** must be defined by its **oversight mandate**. The needs for information of a committee that deals with issues of policy and legality are different to those of a committee mandated to oversee the efficiency of intelligence operations – which requires more in-depth information. This relationship is important not only for providing committees with the information needed to fulfil their mandate, but also for preventing MPs` attempts to access information that may be unrelated to their work. The ***need to know*** principle addresses the same issue: even if someone has all necessary official approvals they should not get access to specific information unless they have a *need to know* that information, 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 Control Panel has the right to request information, documents and other data files from the federal government and the three intelligence services. Demands must be met immediately. Staff of the intelligence agencies can also be questioned. Control Panel's members are sworn to secrecy, they can comment publicly on certain issues, if the decision to do so is reached by two-thirds of its members. Control Panel may request expert witnesses to submit evaluations. (Parliamentary Control Panel Act)
- Romania – The Intelligence Oversight Committee (for the domestic service SRI) can request reports, briefs, explanation, documents, data and information; they can summon military and civilian personnel of the service to hearings. SRI is obliged to submit the information requested to the Committee within 7 working days; if the deadline is overdue SRI is obliged to explain the reasons and say how much time will be needed to prepare the requested information. (Parliament Decision No. 85/2017)
- Hungary – two thirds of National Security Committee can vote to require the executive/an agency to disclose specific information concerning the intelligence agency's methods. (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. 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"[40]: before passing the information to a third party the agency must request permission from the originating entity. There is little data available on how often such requests are made and if they are successful. The sharing of information between intelligence agencies has increased exponentially over the past decade, international cooperation having become one of the main sources of intelligence information. Without information about international intelligence cooperation, committees have an incomplete view of activities involving their own state's agency. Getting more information about international cooperation (or even being exempt from the third party rule) is an endeavour of many oversight bodies in Europe.

[40] sometimes referred to as 'originator control (ORCON)

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

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

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

How can the access to information be improved?

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

3.2. 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 parliament in a democracy; knowledge of oversight tools; familiarity with parliamentary and committee procedures. The work of parliament, the legislative procedures, the function of committees, and their role within the system of checks and balances that make democratic accountability possible is unique, and difficult to grasp for outsiders. Before learning about the particularities of the intelligence world, committee members (especially new MPs) need to understand and internalize the principles and the modalities of democratic oversight, develop the attitude, the political will and the courage necessary for engaging in meaningful oversight activities.

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 infringed upon 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` complaints, and complaints of service employees, including what protections exist for intelligence staff, such as protection from illegal orders or whistleblower 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 UK

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

Investigatory Powers Commissioner's Office (IPCO) constitutes an amalgamation of separate commissioners' offices into one with the passing of the Investigatory Powers Act (IPA) in 2016. IPCO has the responsibility for overseeing the daily intelligence activities of all bodies and agencies exercising investigatory (i.e intelligence gathering) powers. This includes a set of judges (called Judicial Commissioners) who provide the "double-lock" sign-off on interception warrants, as newly mandated by the IPA of 2016. In all, the IPCO comprises:

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

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

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

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

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 interception.[41] The implementation of these legislative provisions will better equip the responsible committee to engage in an informed dialogue with, and undertake more efficient investigations of the overseen institutions. Two practical questions will need to be resolved concerning the implementation of the new law:

- How will the budgetary implications 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 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 employ by the interception oversight committee when needed?

[41] Art. 58 of the Law also makes reference 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

3.3. Committee procedures

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

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

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

- The mandate should describe the issues and/or institutions in the committee`s area of competency. The committee RoP would need to be updated (and voted upon) frequently, at any change of institutional design or name in the committee's area of competency. As the committee develops its expertise and understanding of intelligence networks and activities, they might want to broaden or redefine their mandate and the methods of engaging with overseen institutions.
- The rights and responsibilities of the chairperson, deputies and staff.
- The procedure for calling and running a committee meeting including the size of quorum (important for avoiding blockages from the chairperson if he 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 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 required experts (both for permanent and temporary 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.

3.4. 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 citizen supervision body (see section 2.3.4). 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 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 with 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.** Working together committees can better influence the executive and the intelligence sector. Committees have no power of enforcement; their recommendations are not legally binding on the executive; they have to rely on the force of argument, on publicity and on multi-partisan support to convince the parliament to follow their advice and the executive to comply with their recommendations. When acting together, committees have increased legitimacy and their united voice has considerable political weight.

For these reasons, developing cooperation and complementarity of action between 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 and 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 Citizens Supervision Council (see 2.3.4) 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.

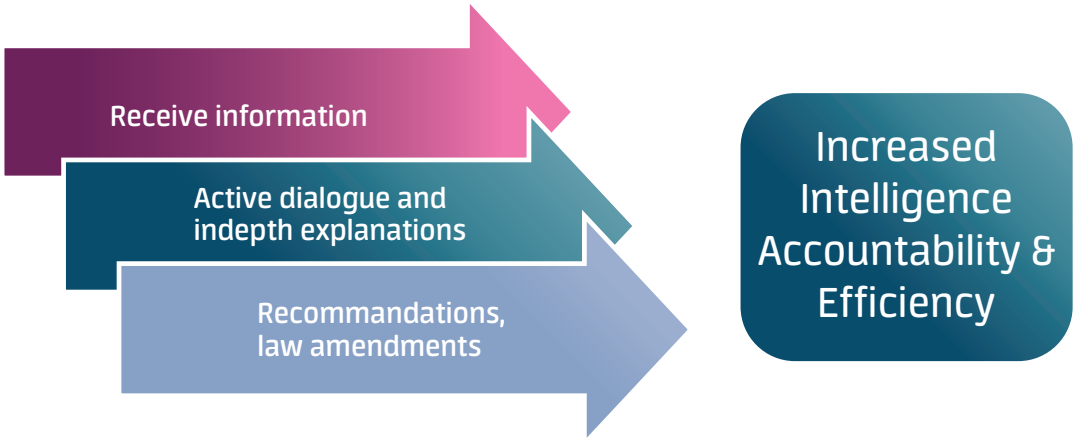
4. COMMITTEE IN ACTION: THE OVERSIGHT TOOLS

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 that they explain and justify 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 problem highlighted in parliamentary debates, media, or complaints received. Committees have the authority to summon ministers, military or civil servants, agency directors or independent experts, in order to answer the committee's questions or even testify under oath.



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

1. Getting information and acquiring a good understanding of the intelligence sector is achieved through 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 for clarification and specific details, and develop their capacity for independent analysis.
3. Having acquired expertise, the committee is better equipped to assess the performance of the security sector, identify weaknesses 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. 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.[42]

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

Regular activity reports[43] 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 providing comprehensive and useful information for oversight, without compromising national security (Australia[44], Canada[45], Croatia[46], Czech Republic[47], Netherlands[48], Romania[49]). 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[50].

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. 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 threat to national and global security, and oversight (substantial and financial) provisions.

- The length can vary from a few concise pages (Netherlands AIVD Annual Report 2016: 12 pages) to a very detailed in-depth report (Australia ASIO Annual Report 2016-17: 146 pages, or Belgium annual report 2016: 227 pages).
- The content[51] may cover, without divulging sensitive details: the annual objectives and priorities of the service; its assessment of major threats to security; any major reforms of intelligence policies, systems, and operations; fulfilment of the reporting and accountability functions of the service; and the response of the service to requests for information under freedom of information legislation.

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 committee to ask accurate and target-oriented questions. The reporting requirements must be sufficient to enable the questions 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 just be as handicapping to effective oversight as too little information.

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

[43] 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.

[44] ASIO Annual Report 2016-17: https://www.asio.gov.au/sites/default/files/Annual%20Report%202016-17.pdf

[45] CSIS Public Report: https://www.csis.gc.ca/pblctns/index-en.php?cat=01

[46] Security-Intelligence Agency 2017: https://www.soa.hr/UserFiles/File/pdf/SOA-Public-Report-2017.pdf

[47] Security Information Service 2015: https://www.bis.cz/vyrocni-zpravaEN890a.html?ArticleID=1104

[48] AIVD Annual Report 2016: https://english.aivd.nl/publications/annual-report/2017/04/04/annual-report-2016

[49] Romanian Intelligence Service Report 2012: https://www.sri.ro/assets/files/reports/2012/REPORT_on_the_Activity_of_the_Romanian_Intelligence_Service_in_2012.pdf

[50] ASIO Annual Report 2016-17, p.135

[51] See Annex 3 for examples of information contained in these reports

What kind of special reports may intelligence oversight committees receive?

Based on legal requirements:

- The Slovenian 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) 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) [52].

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 elaborate tools of oversight.

4.2. Hearings

Hearings can be the most efficient instrument of oversight, if properly used by the parliament. 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. 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[53].

Oversight hearings aim to obtain evidence or in-depth explanations on a specific matter. They are an effective tool for uncovering possible wrongdoings, maladministration, corruption or abuse of power. Government officials are invited to provide information and respond to questions in their area of competency. In most countries, laws and rules of procedure stipulate the obligation of the summoned officials to present themselves in front of the committee and

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

[53] 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).

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.
- Written and oral evidence taken at the hearings is included in the record of the committee. In a number of 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.

The effectiveness of hearings as oversight tool depends on several factors.

1. The independence of the committee in deciding on its hearings 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 of members.
2. Committee's power of investigation
    - In some parliaments the committee's power to summon persons to 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.
    - Sometimes oversight committees may establish an **inquiry (**eventually with the approval of the plenary), but most often, parliament decides to set up an *ad hoc* inquiry committee, with a specific and usually narrow mandate.

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 does not really 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 a 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 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 and 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 point of the visit or having strife within the visiting team. "Perfect planning prevents poor performance"[54]. Good preparation of the visit has distinct 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 like improving the understanding of intelligence processes. Sometimes visits are organised urgently after major incidents, complaints or allegations by citizens, politicians, 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.

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, the context that lead the committee to decide on the visit and its objective. Discussions will cover the location, timing and subject of the intended visit.

- This step proceeds 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 facilities of the services.
- The issues discussed and agreed upon should be written down to avoid confusion and misunderstandings during the visits.

[54] Belgian intelligence review committee

Choice of the sites and items to be visited

The committee decides the site to be visited (headquarters of a service, local or technical installations, etc.) and the specific areas to 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 location of facilities, even if some are classified information.
- A specific agreement must be made 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 locations, but an agreement can be made with the service that all such facilities must be registered in a dedicated file, that 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 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 a general character and specifically relating 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 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 "worse case scenarios" should be considered and mitigated. It can for example happen that access is refused, certain information is refused, strong discussions start with the service representatives, the committee's members do not agree among themselves, visiting procedures are violated, etc.
- In some cases, if the committee has many members, or if the objective of the visit is very narrow, it might be better 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.
- Give an explanation of the mandate and purpose of the visit to the staff receiving the committee. Explain what is required, for example, 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 personnel 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 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 written down by the rapporteurs.
- Objective, unbiased oversight must even in complex and potentially conflictual situations, 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 enter political or 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 proceeding, 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 that the visiting team and/or the whole committee organise a debriefing of the visit.

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-term, medium-term and long-term ones. They can also be distinguished according to the authorities they concern, as in the following exemplifying table.

ITEM	Surveillance of radical groups	Actions to be taken /responsible authority	Timeframe
FINDINGS	1. According to legal mandate	None/ Parliament	_
	2. Absence of operational collection plan	Write collection plan/ service head 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 minister and the visited service should receive 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, of 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 Committee Rules of Procedure describe with detail and clarity how field visits are organised. If not Rules of Procedure, an overall protocol should be agreed at the outset of the 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 better understanding the intelligence organisation, functions and activities. A study visit at headquarters building is the best place to get an overview of operations, administration etc and then move 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 situation.
- 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 although in an "announced visit period", visits can take place after short notice in urgent situations.
- When Committee members have security clearances check that their clearance, and the clearance of accompanying staff are at the necessary level (depending on the objective and topic of the field visit) and that they cover physical access to sites and facilities
- Ensure the services understand the "need to know" 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; the lack of good understanding of legislation and 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. With other words, the summoned officials must provide to the committee documents and information 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[55] (exceptions are found 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. Below are a few examples:

- Germany's "NSA Inquiry" (Untersuchungsausschuss ""NSA")" launched in the Bundestag in March 2014.
- In France and Belgium national parliaments each created a special inquiry committee after the terrorist attacks of 2015 and 2016.
- The Romanian Senate established in 2006 an ad hoc inquiry committee that investigated for two years the existence of CIA secret detention sites on national territory.

What special investigatory powers may committees have?

The Defence Committee in the German Bundestag 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, Parliament must take a decision to this effect. A committee of inquiry is 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.

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 a committee summons or failure to provide the required information (Art.22), prescribing fines that go up to 2.000 Euros for employees and to 20.000 Euros for legal entities.

In practice, however, few inquiries, whether conducted by parliament or judges, have delivered satisfactory results, at least in the area of 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. The information parliament gets is ultimately the information the intelligence services decide to share.

[55] 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.

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.

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 for 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 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's 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[56].

The Annual Activity Report of the intelligence service is usually submitted to the Parliament before being published. The intelligence oversight committees analyze the report and discusses with the service 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 it 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 a 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.[2] 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, initiated investigations and hearings and made frequent press releases.

In the UK the Investigatory Powers Commissioner 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 (such as the number of sessions and hours of work), oversight methods, inter-institutional dialogue, and recommendations[3].

5.2. Assessment of oversight

The main problem in evaluating 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 records of their findings and recommendations and introduce a follow-up system for 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:

[56] 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.

- 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 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 into 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 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, 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 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 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 is 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, and NGO's 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 which 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 usually consider legislation and polices 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 legislative 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 schedules* 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.

ANNEXES

ANNEX A: OVERVIEW OF MACEDONIAN LEGISLATION FOR PARLIAMENTARY OVERSIGHT

CONSTITUTION OF THE REPUBLIC OF MACEDONIA

Art. 68

The Assembly of the Republic of 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 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 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 Macedonia.

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

LAW ON INTERNAL AFFAIRS

UNOFFICIAL CONSOLIDATED VERSION (O.G.42/2014, 116/2014, 33/15, 5/16, 120/16, 127/16, 142/16 and 190/16)

Control from the Parliament of the Republic of Macedonia

Art. 60

The Parliament of the Republic of Macedonia performs control, that is, oversight of the work of the Directorate through an appropiate Committee (hereinafter: the parliamentary Committee).

Program and report on the work of the Directorate submitted to the parliamentary Committee

Art. 61

(1) The Directorate shall submit a program and a report on its work to the parliamentary Committee.

(2) This program shall be submitted by the end of January for the current year, and the report shall be submitted until the end of February reproting on the work in the previous year.

Notifications, data and information that the Directorate provides to the Parliament

Art. 62

(1) Upon request of the parliamentary Committee, the Directorate allows insight and provides the neccessary notifications, data and information from the scope of work of the parliamentary Committee referring to the procedure for performing the activities within the competence of the Directorate.

(2) All data, notifications and information submitted to the parliamentary Committee or presented at a session of the Committee shall be information with an appropriate classification level.

(3) The members of the parliamentary Committee shall be obliged to protect the classified information they have obtained or who have had access during or in connection with the work in the Committee, in accordance with the regulations in the area of classified information.

(4) The obligation for protection of the confidentiality of classified information shall continue after the termination of the function - member of the paliamentary Committee, ie termination of the mandate in the Parliament, in accordance with the regulations in the field of classified information.

Report on the work of the Committee to the Parliament

Art. 63

(1) The parliamentary Committee shall submit a report to the Parliament on the performed work at least once a year.

(2) The Committee report referred to in paragraph (1) of this Article shall be classified information with a degree of classification appropriate to the degree of classification of the report submitted by the Directorate (UBK)

(3) The Parliament submits the conclusions regarding the report of the parliamentary Commission to the Government of the Republic of Macedonia.

LAW ON THE INTELLIGENCE AGENCY

Official Gazette of the Republic of Macedonia no. 19/95

II. OVERSIGHT OF THE WORK OF THE INTELLIGENCE AGENCY

Art. 9

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

LAW ON DEFENCE *(unofficial consolidated version)*

Official Gazette of the Republic of Macedonia no. 42/2001, 58/06, 110/08, 51/11, 151/11, 215/15, Decision of the Constitutional Court 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 Macedonia for exercise and training activities, participation in peacekeeping and humanitarian operations as well as participation of the units of the Armed Forces of the Republic in similar activities abroad;
8) approves a national security and defense concept of the republic;
9) declares the Armed Forces Day and the Civil Protection day;
10) passes 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.

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 Macedonia;
- the Classified Information Security Directorate;
- the Personal Data Protection Directorate and
- the People's 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 A**rticle 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 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 Macedonia shall set up a Committee from the Members of the Assembly of the Republic of 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 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 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 Macedonia for the special investigative measures which will be submitted by the Public Prosecutor of the Republic of Macedonia to the Assembly of the Republic of 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 confirmation 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 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 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 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 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 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

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 Macedonia for a period of 3 years without a right to re-appointment

(2) The Assembly of the Republic of 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 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 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 Macedonia.

(3) When necessary and upon request of the Assembly of the Republic of 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 Macedonia.

(2) The funds for the work of the Council shall be provided from the Budget of the Republic of 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 People's Ombudsman of the Republic of Macedonia

People's Ombudsman of the Republic of Macedonia

Article 56

The People's Ombudsman of the Republic of 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.

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.

COMMITTEE FOR SUPERVISING THE WORK OF THE SECURITY AND COUNTER-INTELLIGENCE DIRECTORATE 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 Security and Counter - Intelligence Directorate and the Intelligence Agency;
- respecting the Law in exercising the authority of the Security and Counter - Intelligence Directorate 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 Security and Counter - Intelligence Directorate 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 Security and Counter - Intelligence Directorate and the Intelligence Agency;
- establishment of international cooperation on issues referring to such supervision and
- other questions regarding the Security and Counter - Intelligence Directorate 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 MANAGEMENT, CUSTOMS MANAGEMENT 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 Management, Customs Management 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 Management, Customs Management 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 Management, Customs Management 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 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 Management, Customs Management and the Ministry of Defence.

ANNEX B: 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 the committee, individual members and 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. The committee can decide whether it should be shared with overseen institutions, the parliament and the public.

Period	Activities	Follow –up
First parliamentary session (February-July)	Annual Activity Reports are debated and approved: 1. UBK 2. Intelligence service (AR) 3. OTA	Activity reports and discussions in the committee with representatives of the service. Recommendations are formulated in writing, and sent to the service after the meeting, with timelines for implementation. Committee Opinions on the intelligence activity are submitted to and 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 classified.
	Oversight hearings: ■ (Two) Proactive – planned in advance, on big policy /reform issues ■ (X) Reactive– to different issues revealed by media, MPs, independent sources. Public officials invited with 24-48 hours notice.	Recommendations. Report on website. Press release.
	(One) Joint meeting with other committee(s) involved in intelligence 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 ■ Two Planned ■ Two Un-planned	

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
	(Four) Oversight Field Visits	Press conference/press release. Committee Opinion delivered to institution visited (submitted as well to the plenary?)
	(Four) 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.

ANNEX C:
TOPICS COVERED BY ANNUAL ACTIVITY REPORTS OF INTELLIGENCE SERVICES

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/tightened as a consequence, to prevent further breaches? *In 2014, Romanian SRI Implemented 44.759 interceptions of communications, of which 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).*
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 on previous year) (SRI 2014 Yearly Activity Report, p.31)*

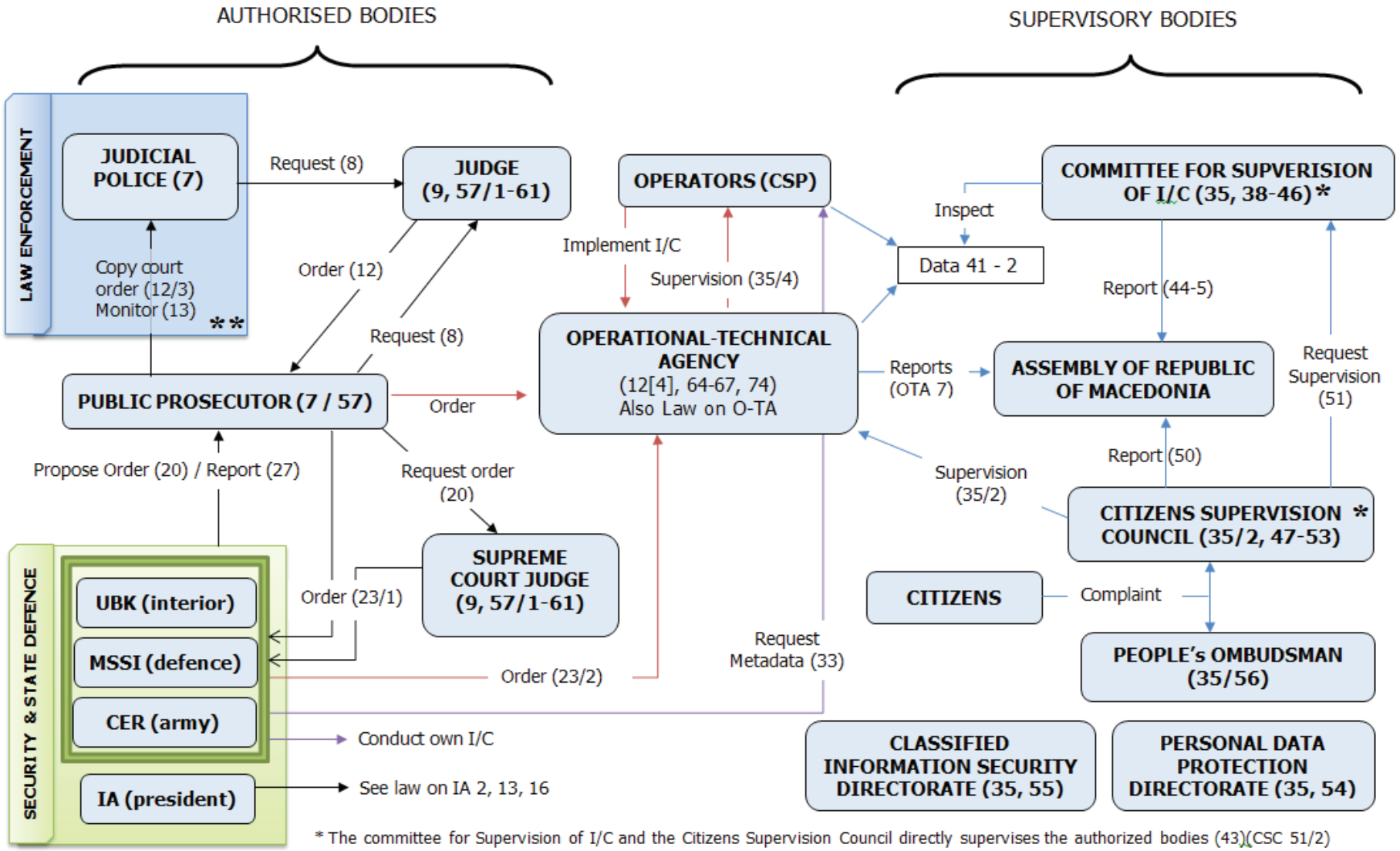
Intelligence reports produced for different beneficiaries	Yearly	Number of reports Number of beneficiaries	What feedback do the beneficiaries send back? Are the reports used in political decision making? How is the service adapting its intelligence products following the feedback? *Croatian SOA has submitted in 2014 approx. 8,700 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 produced a total of 457 intelligence reports in 2016, 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)*
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 breakdown in terms of gender, education, ethnicity age is a useful indicator of diversity.

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 Raport on access to information of public interest 2016)*
Budget – overall amount. Personnel expenses, current expenditures, development and modernisation.	Yearly	Compare with overall amounts from previous years.	Overall amounts are published in public annual activity reports. However, committee should have access to more detailed information on budget execution.
Security Vetting	Yearly	Number of people vetted	Vetting includes access to personal data, therefore it needs to be carried out following transparent procedures; allowing for appeal 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 5,933 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 1,433 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)*
Training / briefing national institutions	Yearly	Delivery 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 with cooperation agreements for the 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 of 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*
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)*

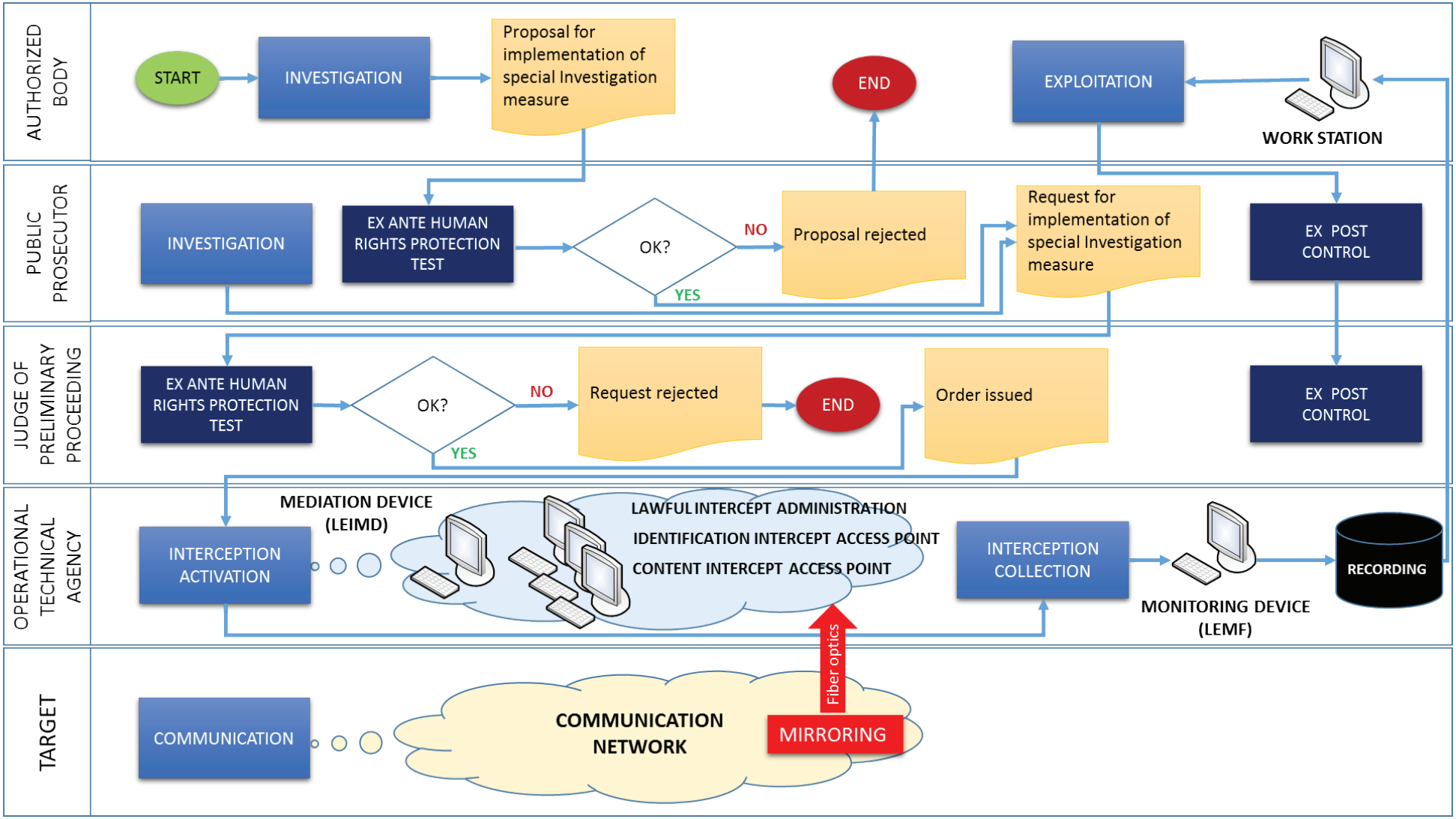
ANNEX D:
ACTORS AND PROCESSES IN COMMUNICATIONS INTERCEPTION IN THE REPUBLIC OF MACEDONIA

Law on Interception of Communications (I/C) Stakeholder connections (Numbers in Graph below are referring to Art. in the Law)

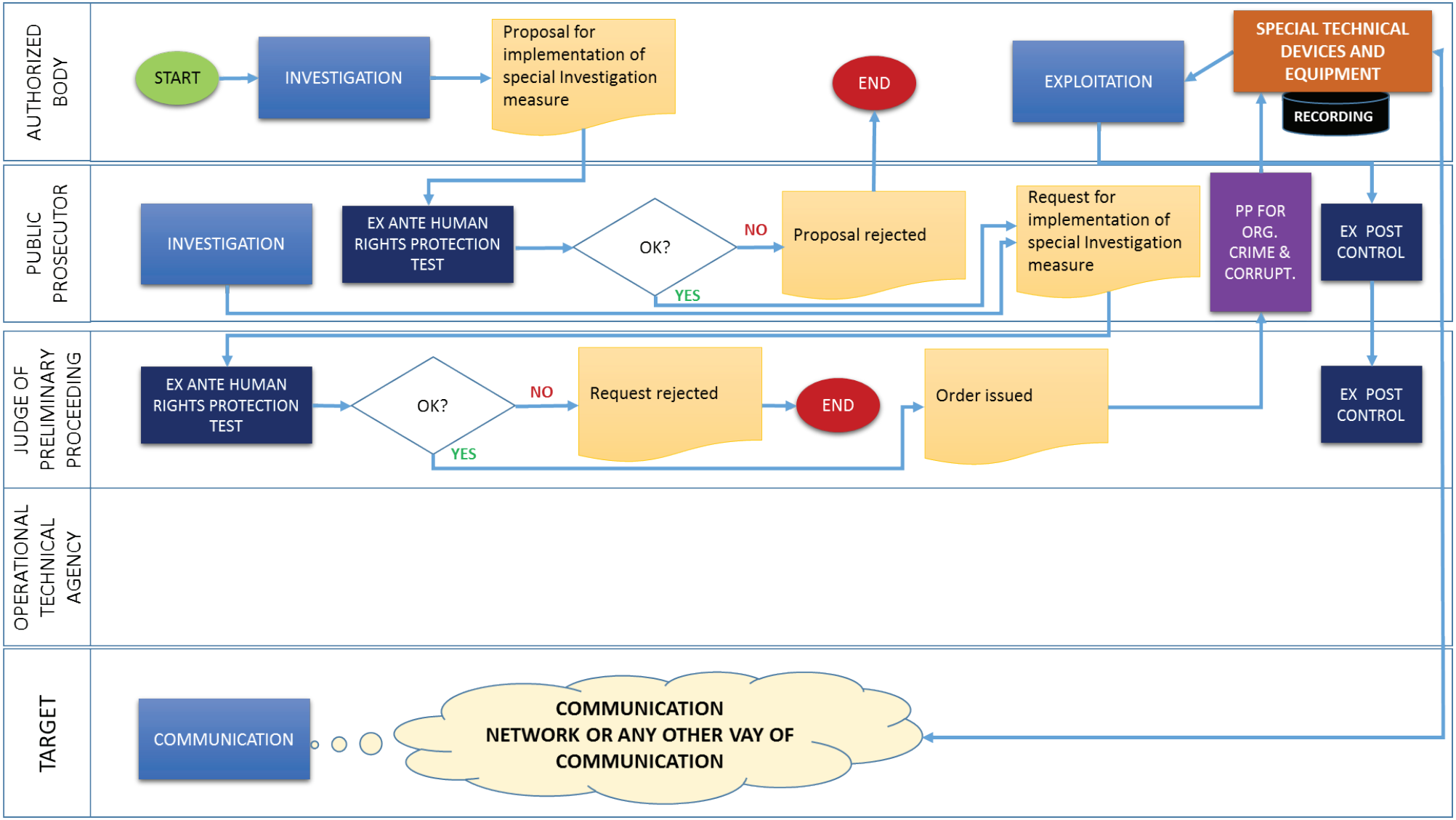


* The committee for Supervision of I/C and the Citizens Supervision Council directly supervises the authorized bodies (43)(CSC 51/2)
** Other authorised bodies of law enforcement: customs administration, financial police

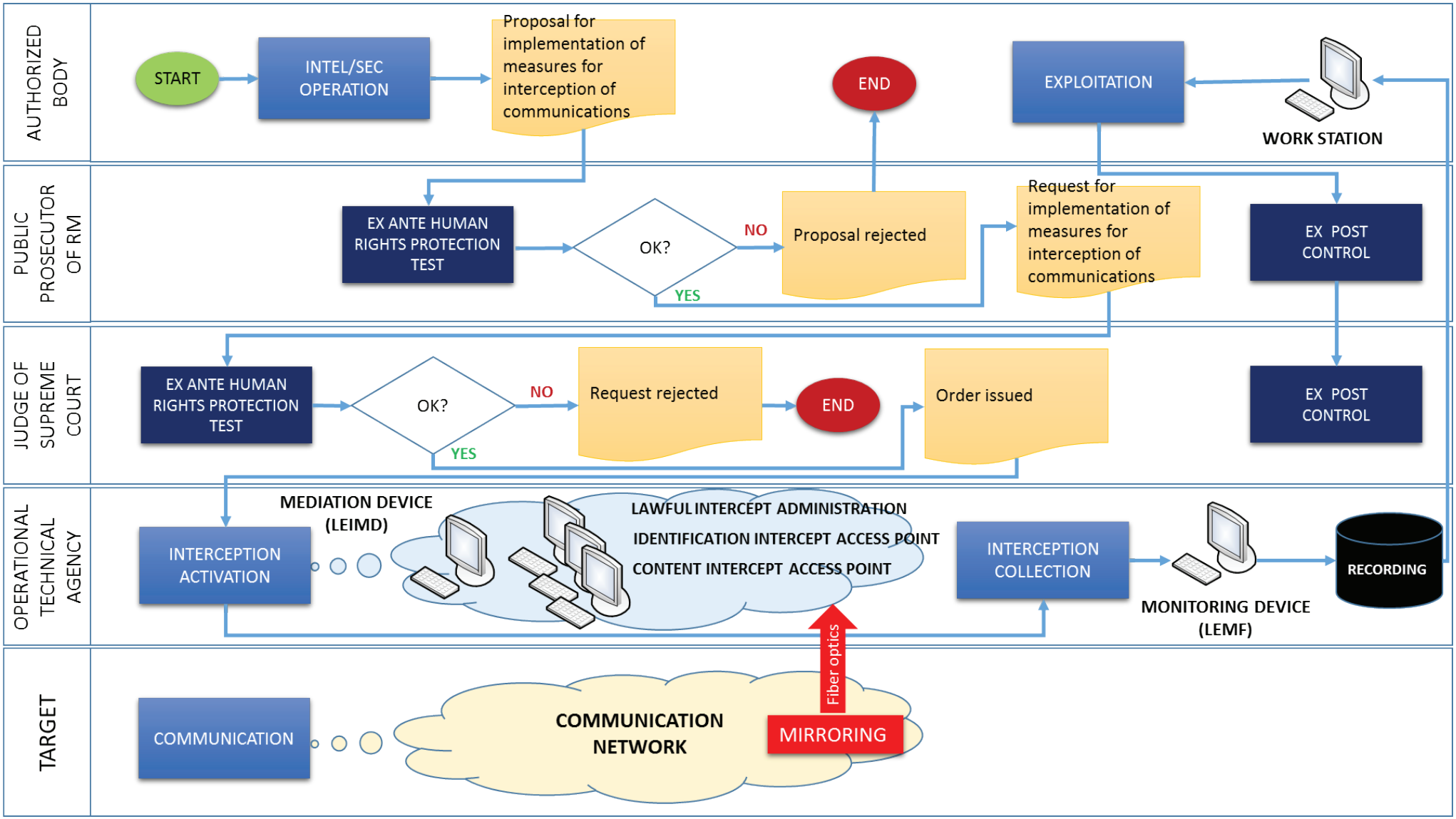
Interception of Communications in criminal investigation WITH mediation of OTA



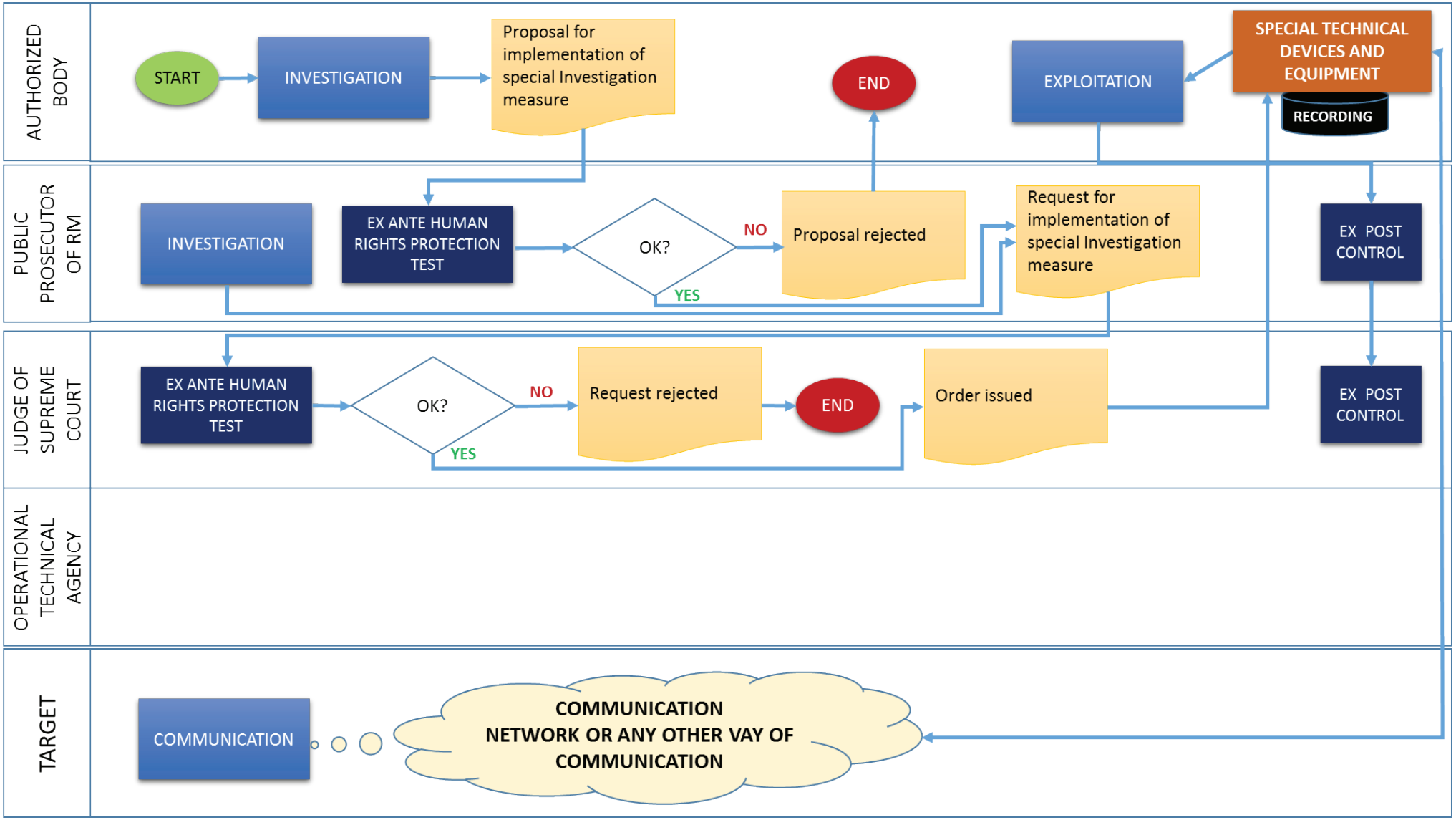
Interception of Communications in criminal investigation WITHOUT mediation of OTA



Interception of Communications in intelligence and security operations WITH mediation of OTA



Interception of Communications in intelligence and security operations WITHOUT mediation of OTA



DCAF

a centre for security,
development and
the rule of law

The Geneva Centre for the Democratic Control of Armed Forces (DCAF) promotes good governance and reform of the security sector. The Centre conducts research on good practices, encourages the development of appropriate norms at the national and international levels, makes policy recommendations and provides in-country advice and assistance programmes. DCAF's partners include governments, parliaments, civil society, international organisations and the range of security sector services, including the military, police, judiciary, intelligence agencies, and border security services.

Visit us at www.dcaf.ch