3.1 Toolkit – Legislating for the Security Sector

Guidebook

Understanding Intelligence Oversight

Aidan Wills

Geneva Centre for the
Democratic Control of
Armed Forces (DCAF)

Guidebook

Understanding Intelligence Oversight

Aidan Wills

Geneva Centre for the
Democratic Control of
Armed Forces (DCAF)

About DCAF

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 security sector actors such as police, judiciary, intelligence agencies, border security services and the military.

Further information on DCAF is available at:
www.dcaf.ch

Acknowledgements

DCAF would like to thank the members of the Editorial Board for their dedication and the time they devoted to review this series.

Furthermore, DCAF would like to thank Beverly Youmans and Stephanie Chaban for their editorial assistance.

Publisher

Geneva Centre for Democratic Control of Armed Forces (DCAF).

Cover picture © REUTERS/ Chris Wattie, 2007

ISBN: 978-92-9222-131-7

Editorial Board

The Editorial Board for the series of booklets on intelligence oversight comprises:

- Hans Born, Geneva
- Ian Leigh, Durham
- Arnold Luethold, Geneva
- Benjamin Buckland , Geneva

TABLE OF CONTENTS

Introduction to the Toolkit 8

Understanding Intelligence Oversight 10

- What is the aim of this guidebook? 10
- What does this guidebook contain? 10
- Who is this guidebook for? 10
- What are intelligence services? 10

Intelligence services in a democratic society 11

- What is the role of civilian intelligence services in a democratic society? 11
- What is the role of military intelligence services? 11

Legal framework for intelligence services 13

- How do democratic societies provide a legal basis for intelligence services? 13
- Why do intelligence services need a legal basis? 13
- Are intelligence laws secret? 14
- What do intelligence laws cover? 14
- How do democratic societies ensure intelligence services uphold the law? 15
- What are the international legal standards guiding intelligence services? 15
- Are intelligence services permitted to violate human rights? 15

Information collection 17

- How do intelligence services collect information? 17
- What information are intelligence services permitted to collect? 17
- What information are intelligence services not permitted to collect? 18
- Why do states restrict the collection of information from certain professions? 18
- How does a democratic society control the use of special powers? 18
- Who authorises the use of special powers? 18
- How does the state authorise the use of special powers? 19
- How do democratic societies oversee the use of special powers? 19

Use and management of personal data 21

What is personal data? 21

How do intelligence services acquire personal data? 21

How do intelligence services and their governments use personal data? 21

Why do democratic societies restrict the use of personal data? 22

What legal controls apply to the use of personal data? 22

Who oversees the use of personal data and what do they do? 23

Can individuals access their personal data? 24

International intelligence cooperation 25

What is international intelligence cooperation? 25

Why do intelligence services cooperate with foreign governments and intelligence services? 25

What are the risks of intelligence cooperation? 25

How do states control international intelligence cooperation? 26

What controls apply to the sharing of information with foreign intelligence services? 26

How is international intelligence cooperation overseen? 27

The intelligence services' use of powers of arrest and detention 27

Should intelligence services have powers to arrest and detain individuals? 27

What international standards apply to the use of powers of arrest and detention? 28

Do intelligence services need their own detention facilities? 28

The use of lethal force by intelligence services 28

Are intelligence services permitted to kill? 28

The control and oversight of intelligence services 31

Why do democratic societies control their intelligence services? 31

Which institutions control and/or oversee intelligence services? 32

Internal management 32

What role does internal management play in controlling intelligence services? 32

To whom do intelligence services report? 32

Who appoints directors of intelligence services? 32

Why are directors of intelligence services appointed for a fixed period? 33

The executive 33

What role does the executive play in controlling intelligence services? 33

The judiciary 33

What is the role of the judiciary in controlling and overseeing intelligence services? 33

Parliament 34

What is the role of parliament in controlling and overseeing intelligence services? 34

Expert oversight bodies 34

What is the role of expert intelligence oversight bodies? 34

An in-depth study of parliamentary and expert intelligence oversight bodies 38

Which aspects of intelligence services' work are overseen by parliamentary and/or expert oversight bodies? 38

What legal powers do oversight bodies have? 38

Why do oversight bodies need financial and human resources? 39

How do overseers monitor intelligence services? 39

How do oversight bodies report on their activities? 40

Why are public reports important? 40

Is there a conflict between the right to know and the need to keep information secret? 40

How can the information needs of oversight bodies and intelligence services be reconciled? 40

Why is the relationship between intelligence services and oversight bodies important? 41

How do democratic societies ensure the independence of intelligence oversight bodies? 41

How can the independence of members of oversight bodies be ensured? 42

What are the advantages of parliamentary oversight bodies? 42

What are the advantages of expert oversight bodies? 42

Complaints about intelligence services 43
How can the public complain about intelligence services? 43
Which institutions handle complaints about the intelligence services? 45
Why do some states notify people when special powers have been used against them? 45
What makes a complaints-handling body effective? 46
Further reading 47
Endnotes 48

List of Tables and Boxes

Table 1: Examples of the mandates and functions of intelligence services 12
Table 2: A comparison of selected intelligence oversight bodies in Belgium, Canada, South Africa and the United Kingdom 35

Box 1: South African constitutional provisions on the intelligence and security services 13
Box 2: Extract from Common Article 3 of the Geneva Conventions 16
Box 3: The process for authorising the use of special powers by the Canadian Security Intelligence Service 20
Box 4: Regulations on the use of personal data by the German Federal Office for the Protection of the Constitution 23
Box 5: German law on access to personal data held by intelligence services 24
Box 6: Croatian regulations on intelligence cooperation with foreign entities 27
Box 7: International standards on arrest and detention 29
Box 8: International standards on the use of force by public officials 31
Box 9: Complaints-handling by Canada's Security Intelligence Review Committee (SIRC) 44
Box 10: German law on notifying individuals after special powers have been used against them 45

Introduction to the Toolkit

Legislating for the security sector is a complex and difficult task. Many lawmakers thus find it tempting to copy legislation from other countries. This expedites the drafting process, especially when the texts are available in the language of the lawmaker, but more often than not, the result is poor legislation.

Even after being amended, the copied laws are often out of date before coming into effect. They may no longer be in line with international standards or they may not fully respond to the requirements of the local political and societal context. Copied laws are sometimes inconsistent with the national legislation in place.

In some cases, there is simply no model law available in the region for the type of legislation that is needed. This has been the case in the Arab region, where the security sector has only slowly begun to be publicly debated. It is thus difficult to find good model laws for democratic policing or for parliamentary oversight of intelligence services.

It is therefore not surprising that many Arab lawmakers have felt frustrated, confused, and overwhelmed by the task of drafting legislation for the security sector. They found it difficult to access international norms and standards because little or no resources were available in Arabic. Many of them did not know where to search for model laws and several were about to give up. Some eventually turned to DCAF for assistance.

The idea of a practical toolkit for legislators in the Arab region came when practitioners began looking for a selection of standards, norms and model laws in Arabic that would help them draft new legislation. Experts from the Arab region and DCAF thus decided to work together and develop some practical tools.

Who is this toolkit for?

This toolkit is primarily addressed to all those who intend to create new or develop existing security sector legislation. This includes parliamentarians, civil servants, legal experts and nongovernmental organisations. The toolkit may also be helpful to security officials and, as a reference tool, to researchers and students interested in security sector legislation.

What is in the toolkit?

The bilingual toolkit contains a number of booklets in English and Arabic that provide norms and standards, guidebooks as well as practical examples of model laws in various areas of security sector legislation.

The following series have been published or are being processed:

- Police legislation
- Intelligence legislation
- Military Justice legislation
- Status of Forces Agreements

Additional series will be added as the needs arise. The existing series can easily be expanded through the addition of new booklets, based on demand from the Arab region.

For the latest status of publications please visit: www.dcaf.ch/publications

What is the purpose of this toolkit?

The toolkit seeks to assist lawmakers in the Arab region in responding to citizens' expectations. Arab citizens demand professional service from police and security forces, which should be effective, efficient and responsive to their needs. They want police and security organisations and their members to abide by the law and human right norms and to be accountable for their performance and conduct. The toolkit thus promotes international standards in security sector legislation, such as democratic oversight, good governance and transparency.

The toolkit offers easy access in Arabic and English to international norms as well as examples of legislation outside the Arab region. This allows to compare between different experiences and practices.

The scarcity of Arab literature on security sector legislation has been a big problem for Arab

lawmakers. The toolkit seeks to address this deficiency. One of its aims is to reduce time lawmakers spend on searching for information, thus allowing them to concentrate on their main task. With more information becoming available in Arabic, many citizens and civil society groups may find it easier to articulate their vision of the type of police and security service they want and to contribute to the development of a modern and strong legal framework for the security sector.

Why is it important to have a strong legal framework for the security sector?

A sound legal framework is a precondition for effective, efficient and accountable security sector governance because it:

- Defines the role and mission of the different security organisations;
- Defines the prerogatives and limits the power of security organisations and their members;
- Defines the role and powers of institutions, which control and oversee security organisations;
- Provides a basis for accountability, as it draws a clear line between legal and illegal behaviour;
- Enhances public trust and strengthens legitimacy of government and its security forces.

For all these reasons, security sector reform often starts with a complete review and overhaul of the national security sector legislation. The point is to identify and address contradictions and the lack of clarity regarding roles and mandates of the different institutions.

Understanding Intelligence Oversight

What is the aim of this guidebook?

This guidebook provides an introduction on how democratic states govern their intelligence services. It demonstrates how states can govern their intelligence services in order to make sure that:

a. They contribute effectively to the security of the state and its population,

b. They are subject to democratic control,

c. They are accountable to the populations they serve, and

d. They respect the rule of law and human rights.

The guidebook provides short and simple answers to frequently asked questions on the activities of intelligence services, as well as the control and oversight of these organisations. It draws extensively on the laws, institutional models and practices of a wide range of democratic states. This guidebook also illustrates that democratic states differ in their approaches to organising, tasking and overseeing their intelligence services. There is no one "right" model or approach. There are however, widely accepted good practices on the activities and oversight of intelligence services which apply in many democratic states – this guidebook outlines many of these.

What does this guidebook contain?

The guidebook is divided into seven sections. The first focuses on the role intelligence services play in democratic societies. The following section looks at some main features of legal frameworks that regulate intelligence services. Four sections are devoted to explaining how democratic states control the activities of their intelligence services in intelligence collection, the use and management of personal data and international cooperation. The final section of this guidebook focuses on the control and oversight of intelligence services by the executive, parliament, judiciary and expert oversight bodies.

Who is this guidebook for?

This guidebook is for people interested in the governance of intelligence services, but who do not have an expert understanding of the subject. More specifically, this guidebook addresses three main groups. First, it is for those involved in developing laws and institutions for governing intelligence services. This includes parliamentarians and their staffers, members of the executive, staff from intelligence services, and representatives of civil society organisations. Second, this guidebook is for members and staffers of newly established oversight bodies. Finally, this guidebook hopes to meet the needs of teachers and students who wish to have a general introduction to intelligence governance.

The material in this guidebook is presented in a descriptive way, in the form of a series of simple questions and answers. This format should assist non-expert practitioners in applying and using the material for their own needs.

What are intelligence services?

This guidebook refers to intelligence services as government organisations, whose main tasks are the collection and analysis of national security related information, and its dissemination to decision makers. This information typically concerns threats to national security such as terrorism, the proliferation of weapons of mass destruction, and espionage by hostile states.

In most democratic states, these tasks are performed by a specialised intelligence service. However, in some countries such tasks are performed by a branch of the police.

States often mandate their intelligence services to work exclusively within or outside the borders of their state. Accordingly, they may have different intelligence services to work at home and abroad. Other states mandate one intelligence service to work both within and outside the national boundaries. While this guidebook focuses primarily on domestic intelligence services,

defined as intelligence services that work within the territory of their state, the underlying principles for oversight and control apply equally to intelligence services that operate abroad.

Intelligence services in a democratic society

What is the role of civilian intelligence services in a democratic society?

Intelligence services are an important part of the security sector in a democratic society. Their primary function is to collect and analyse information about threats directed against the state and its population. They provide this information to the government, enabling it to develop and enforce security policy. It is not however, the role of intelligence services to enforce security policy. This is the responsibility of the police and other law enforcement agencies.

The information collection role of intelligence services is limited; their investigations focus only on activities posing a threat to national security. They do this in accordance with legislation and the government's political guidance. Society, not intelligence services, defines what constitutes a threat to national security. This is usually a lengthy process which results in the formulation of a national security policy or legislation.

Intelligence services perform other tasks in addition to their information collection role. For example, they do counter-intelligence activities. These activities include detecting and disrupting espionage conducted by foreign intelligence services that is directed against the interests of the state and its population. Additionally, intelligence services are often responsible for protecting the state's information and information systems. For example, they screen applicants for government jobs that would give those individuals access to classified information. (See Table 1 for details of the mandates and functions of selected intelligence services).

The role of intelligence services is essential for protecting both the state and its population. National law prohibits intelligence services from promoting or protecting the special interests of any particular religious, ethnic or other group. They remain impartial in their role to serve all individuals in the society. By preventing terrorism and other threats to national security intelligence services contribute to the safety and well being of all individuals in the society.

What is the role of military intelligence services?

Military or defence intelligence services are part of the armed forces. In democratic societies, their mandates are more limited than those of civilian intelligence services. They are primarily responsible for collecting and analysing information about threats to armed forces personnel and bases, and for sharing such information with the senior military command and the political leadership. The potential threats that military intelligence services need to monitor may originate from within the armed forces, domestic groups, or from foreign states and entities. In many states, military intelligence services are also tasked with protecting sensitive defence-related information and communication systems. Military intelligence services may operate both domestically and abroad, depending on a country's needs, its legislation, and its force deployment.

Democratic societies do not permit their military intelligence services to gather information about threats to security that are not defence related. Collecting information on non-military threats is the responsibility of civilian intelligence services. Thus, military intelligence services are normally not permitted to collect information on civilians in their own state. In many states, the law requires military intelligence services to call upon the civilian intelligence service if they need to gather information about threats to the armed forces posed by civilians. This restriction is designed to prevent armed forces from interfering in civilian affairs.

Table 1: Examples of the mandates and functions of intelligence services[1]

Country	Mandates and functions of the civilian intelligence services
Canada	• The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada. • The Service may provide security assessments to departments of the Government of Canada. • The Service may: a. advise any minister of the Crown on matters relating to the security of Canada, or b. provide any minister of the Crown with information relating to security matters or criminal activities, that is relevant to the exercise of any power or the performance of any duty or function by that Minister under the Citizenship Act or the Immigration and Refugee Protection Act.
Croatia	• Systematic gathering, analysis, processing and evaluation of information relevant for the national security; • With the aim of detecting and preventing activities, by individuals or groups, directed: against the viability, independence, integrity and sovereignty of the Republic of Croatia, aiming at the violent overthrow of the state authority structures; threatening to violate human rights and basic freedoms established by the Constitution and the legislation of the Republic of Croatia, and to endanger the fundaments of the economic system of the Republic of Croatia.
The Netherlands	• Conducting investigations regarding organisations that, and persons who, because of the objectives they pursue, or through their activities give cause for serious suspicion that they are a danger to the continued existence of the democratic legal system, or to the security or other vital interests of the state. • Conducting security clearance investigations as referred to in the Security Investigations Act; • Promoting measures […] for the protection of information that is to remain secret for reasons of national security, and information pertaining to those parts of the public service and business community that in the opinion of the relevant Ministers are of vital importance for the continued existence of the social order; • Conducting investigations regarding other countries concerning subjects designated by the Prime Minister, Minister of General Affairs, in accordance with the relevant Ministers.

Legal framework for intelligence services

How do democratic societies provide a legal basis for intelligence services?

Some democratic states include general provisions on intelligence services in their constitutions. These constitutional rules are normally general provisions, such as the requirements that intelligence services are accountable to parliament and respect the rule of law (see Box 1 for the South African constitutional provisions on intelligence and security services).

Most democratic states have specific legislation on intelligence services, which forms the primary legal basis for regulating intelligence activities. Laws on privacy, data protection, the security of information, and access to information also provide important regulations for intelligence services. On top of this, the executive issues so called "executive orders", "directives" and other regulations which supplement legislation. Such regulations are always based on existing legislation, and therefore need to comply with it.

Why do intelligence services need a legal basis?

Democratic societies make sure that intelligence services operate in accordance with national laws. A legal basis for intelligence services is important for four main reasons.

First, the law clearly defines the mandate, role and responsibilities of intelligence services and their officials. Laws also define the activities they are permitted to perform. Governments depend on the law in order to control intelligence services.

Second, a legal basis for all government organisations is essential for promoting transparency. Public laws make society aware of the functions and powers of the government. Intelligence services have a legal basis for carrying out special powers to collect information that is not generally available to other government agencies or private individuals. For example, laws may permit them to use particular measures for investigating individuals. Individuals need to know how intelligence services can affect their personal lives and whether intelligence officers are respecting individual rights under the law.

Box 1: South African constitutional provisions on the intelligence and security services[2]

The Constitution of the Republic of South Africa includes a number of general provisions on the intelligence and security services.

- National security must be pursued in compliance with the law, including international law.
- National security is subject to the authority of Parliament and the national executive.
- The security services must be structured and regulated by national legislation.
- The security services must act, and must teach and require their members to act, in accordance with the Constitution and the law, including customary international law and international agreements binding on the Republic.
- Neither the security services, nor any of their members, may, in the performance of their functions
  a. prejudice a political party interest that is legitimate in terms of the Constitution; or
  b. further, in a partisan manner, any interest of a political party.
- To give effect to the principles of transparency and accountability, multi-party parliamentary committees must have oversight of all security services in a manner determined by national legislation or the rules and orders of Parliament.
- National legislation must regulate the objects, powers and functions of the intelligence services.

Third, a legal basis gives intelligence services legitimacy in the eyes of the public. A publicly available law promotes an understanding of what the roles of the intelligence services are, and why they require public money to perform these tasks. This can help to ensure public support for the intelligence services.

Finally, public intelligence laws are needed to hold the government accountable. Intelligence oversight bodies and the public at large hold the executive and intelligence services to account for their compliance with such laws. Public laws also enable individuals to seek justice if they believe intelligence services have committed illegal actions against them.

Are intelligence laws secret?

In democratic states, the fundamental laws governing intelligence services are in the public domain. As discussed on page 13, the public needs to know what the roles of the intelligence services are, and what powers they have for performing these tasks. Members of the public also need to know when and under what conditions the intelligence services would be allowed to restrict individual rights for national security purposes. Therefore, intelligence services' authority to restrict human rights must be contained in public laws.

The government may however, issue "subsidiary regulations" – such as "decrees" and "ministerial instructions" – that are not made available to the public. The law authorises the government to issue such regulations when it believes that making specific information available to the public could jeopardise the work of intelligence services and/or national security more generally. Regulations that are not made public typically contain information related to the operational methods of intelligence services, such as their use of particular devices or technologies. Such information is often not made public because it could give persons knowledge that could enable them to avoid detection by intelligence services, or to uncover persons working for services. This may undermine the effectiveness of intelligence services, pose a threat to the safety of people working for them, and may ultimately harm national security.

Regulations that are not made public must still comply with existing public laws and the constitution. For example, they cannot authorise intelligence services to take actions violating human rights under international law.

What do intelligence laws cover?

Intelligence laws allow states to regulate and oversee intelligence services. These laws cover the following areas. First, intelligence laws outline the mandate of intelligence services and provide a comprehensive list of their tasks. The mandate normally contains definitions of what constitutes a threat to national security. These laws limit the role of intelligence services in order to prevent intelligence officers from promoting interests other than those of the state and its population.

Second, intelligence laws provide a comprehensive list of the powers available to the intelligence services, and regulate how such powers can be used. Laws only permit intelligence services to use these powers in the context of their mandate. They limit the use of powers that may result in restricting individual rights for national security purposes.

Third, intelligence laws describe the structure and composition of intelligence services including the organisational responsibilities of divisions within the services.

Fourth, intelligence laws outline how governmental and non-governmental entities oversee intelligence services. For example, they regulate the process for appointing senior intelligence managers, and outline the mandates and powers of parliamentary and expert oversight bodies.

Fifth, intelligence laws describe the professional relationships intelligence services have with other governmental and non-governmental organisations and international organisations. For example, laws describe the processes the intelligence services use to exchange information or conduct joint operations with other organisations.

Sixth, intelligence laws often provide regulations guiding the use of personal data by intelligence services (see pages 21-25).

Finally, intelligence laws describe the processes individuals use if they want to make complaints about intelligence services' actions taken against them (see pages 43-46).

How do democratic societies ensure intelligence services uphold the law?

Intelligence services, like all other government agencies, are required to respect both international and national law. Of particular importance, are provisions of international human rights law and international humanitarian law. A state's national law on intelligence services must be compatible with its international legal obligations.

All intelligence services and their staff are required to comply with the law. The executive must also act in accordance with the law. The political authorities are not permitted to issue orders to the intelligence services that would require them to take illegal action.

Members of the executive are legally responsible for directives issued to intelligence services. Employees of intelligence services are individually responsible for ensuring that their own actions comply with the law. In many states, the law not only requires them to make sure that their actions comply with the law but also obliges them to disobey orders which would violate national or international law. Thus, a member of an intelligence service would have to answer for his or her unlawful behaviour and could face legal prosecution, even if it had been ordered by a superior. Given the extensive powers that can be given to members of intelligence services, such individual responsibility is particularly important as a safeguard against serious crimes, including human rights violations such as torture and extrajudicial killings.

It is therefore, critically important that the judiciary holds intelligence officers and, if required, members of the executive accountable under the law. Their individual decisions and actions can be challenged in a court; the rulings of a court are binding on the executive, as well as the intelligence services and their staff.

What are the international legal standards guiding intelligence services?

As an institution of the state, intelligence services must comply with the government's international legal obligations. The state's obligations under international human rights law, in particular the civil and political rights outlined in the UN Charter and the International Covenant on Civil and Political Rights, apply to intelligence services. These include the rights to life, liberty, fair trial, privacy and freedom of expression and association.

International standards on law enforcement activities are also relevant to intelligence services if national law permits them to perform law enforcement tasks such arrest and detention.

In 2009 and 2010 the UN reviewed existing international legal standards and institutional controls applying to intelligence services. The UN Human Rights Council mandated a study of good practices on the legal and institutional frameworks for intelligence services and their oversight. This study compiled 35 noteworthy international practices and was presented to the Human Rights Council in June 2010 (see list of references).

Are intelligence services permitted to violate human rights?

International human rights law does not permit states (including their intelligence services) to violate the human rights of anyone under their jurisdiction. In common with all government agencies, intelligence services must comply with international human rights law. In situations of armed conflict, intelligence services must also comply with international humanitarian law. States ensure that these international legal standards are implemented in their domestic law.

International human rights law establishes three categories of human rights and freedoms:

(1) Rights that can never be limited or derogated from in any circumstances;

(2) Rights that can be limited for specific reasons and in accordance with strict legal criteria;

(3) Rights that can be suspended or limited during an armed conflict or state of emergency which threatens the existence of the state.

1. Human rights that can never be limited or derogated from

International human rights law prohibits states and their agencies from limiting or derogating from certain human rights in any situation. These

include the right to life, freedom from torture and other inhuman or degrading treatment, the right to fair trial, the right to recognition before the law, freedom from slavery and involuntary servitude, and the prohibition on abduction and unacknowledged detention.[3] International humanitarian law supplements and reinforces these prohibitions in times of armed conflict; common article 3 of the Geneva Conventions outlines these minimum standards (see Box 2). Intelligence services are not permitted to take any action that infringes upon these rights at any time.

Box 2: Extract from Common Article 3 of the Geneva Conventions[4]

In the case of armed conflict not of an international character occurring [..] each Party to the conflict shall be bound to apply, as a minimum, the following provisions:

1. Persons taking no active part in the hostilities, including members of armed forces who have laid down their arms and those placed "hors de combat" by sickness, wounds, detention, or any other cause, shall in all circumstances be treated humanely, without any adverse distinction founded on race, colour, religion or faith, sex, birth or wealth, or any other similar criteria. To this end, the following acts are and shall remain prohibited at any time and in any place whatsoever with respect to the above-mentioned persons:

    a. violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture;

    b. taking of hostages;

    c. outrages upon personal dignity, in particular humiliating and degrading treatment;

    d. the passing of sentences and the carrying out of executions without previous judgment pronounced by a regularly constituted court, affording all the judicial guarantees which are recognized as indispensable by civilized peoples.

2. Human rights that may be limited

International human rights law permits states to limit certain human rights and freedoms of given persons. These include the rights to liberty, and privacy, and the freedoms of movement, association and expression. States can only take measures that limit the exercise of rights if such measures comply with the following criteria:

1. based on law that is public;
2. pursue a legitimate purpose (such as to protect national security, public safety or the human rights and freedoms of others);
3. be necessary in a democratic society;
4. proportionate to stated aims;
5. consistent with other human rights obligations. States violate the human right in question if they fail to comply with these requirements.

In many states, the law authorises intelligence services to limit the right to privacy by giving them special powers to collect information from/about individuals or groups suspected of involvement in specific activities that threaten national security, public safety and human rights (see pages 17-18). These special powers include measures like monitoring a person's communications without their knowledge or secretly filming their activities. Such measures clearly limit a person's right to privacy. Some states also mandate their intelligence services to perform law enforcement functions (see page 28). In this context, national law gives them the power to arrest and detain persons who are suspected of having committed specific crimes. These powers limit the rights to liberty and freedom of movement.

Democratic states impose strict controls on their intelligence services' use of these powers in order to make sure they comply with international standards. They ensure that such powers are regulated by law, authorised and overseen by institutions outside the intelligence services (see pages 19-21).

3. Derogating from human rights obligations during a state of emergency

International human rights law permits states to temporarily derogate from some of their human rights obligations during a state of emergency. A state may proclaim a state of emergency in exceptional circumstances where the "life of the nation" is threatened. This includes serious and imminent threats to the physical security of the population and/or the functioning of democratic institutions.[5] The decision to declare a state of emergency and to derogate from specific rights is taken by the executive. Intelligence services are not involved in this process.

Upon announcing a state of emergency, a state must notify the relevant treaty body and specify which human rights will be suspended or limited. Suspensions or limitations of specific rights must be temporary, strictly necessary for dealing with the emergency, and proportionate to the threat faced. In addition, any suspensions or limitations of rights must be subject to the review of the judiciary and parliament. States are not permitted to derogate from any of the non-derogable rights mentioned above, or any other non-derogable rights listed in regional and international human rights treaties. Accordingly, national constitutional provisions on emergency powers cannot be used to justify actions that violate international human rights law.

If intelligence services are given additional powers to restrict human rights during a state of emergency, they must continue to comply with both international and domestic human rights law. Their activities must remain under the control and oversight of the executive, parliament, the judiciary, and any expert oversight bodies that exist.

Information collection

How do intelligence services collect information?

In democratic societies intelligence services collect much of the information they need to fulfil their mandate from public sources such as media articles, reports provided by governmental and non-governmental organisations and academic publications. Intelligence services also collect information from persons who have (or could gain) access to relevant information. For example, members of groups that threaten national security may act as informers by secretly passing information to intelligence services. Intelligence services may also use persons with aliases or false identities to infiltrate organisations and provide information about their activities.

Individuals and groups who are planning to threaten national security do not usually disclose their intentions. Consequently, democratic societies need legislation enabling the intelligence services to gather information that cannot be found in the public domain. Thus, legislation gives the intelligence services special powers that are not usually available to other members of society. These special powers fall into four main areas.

First, legislation may permit intelligence services to monitor an individual's verbal, electronic and paper-based communications without their consent. Such activities can require highly developed and complex technical means.

Second, legislation may also allow intelligence services to secretly film and photograph individuals and their property without their consent.

Third, legislation may permit intelligence services to give false identities to its agents to allow them to infiltrate groups which threaten national security.

Finally, legislation may allow them to make official requests to other government agencies or private companies for information about people even when it may infringe on their right to privacy. For example, they may sometimes be allowed to request an individual's phone records from a telecommunications provider.

What information are intelligence services permitted to collect?

In democratic societies, national laws control the information that intelligence services are permitted to collect. Laws permit intelligence services to collect information about specific activities posing a threat to national security, as defined in their legal mandate. They are only permitted to collect information about individuals and groups engaged in such activities if the information is relevant and necessary for carrying out their mandate.

What information are intelligence services not permitted to collect?

Intelligence laws restrict what types of information intelligence officers are permitted to collect. First, laws prohibit them from collecting information about individuals and activities posing no threat to national security

Second, in a democratic society laws usually prohibit intelligence officers from collecting information about lawful political and social activities. For example, they are not permitted to collect information about the lawful activities of political parties and their members, or about groups involved in peaceful protests. These legal prohibitions protect human rights and other values democratic societies consider important, such as the freedoms of association and assembly.

Finally, laws usually prohibit intelligence officers from collecting information for promoting particular interests. For example, the law does not permit them to spy on the political opponents of a particular party.

Why do states restrict the collection of information from certain professions?

Members of some professions such as journalists, parliamentarians, lawyers, clergy and medical doctors have information which may be of interest to the intelligence services. However, many democratic societies have adopted laws and measures to restrict or prevent intelligence services from collecting information from or about individuals from these professions. For example, the law may prohibit collecting information about these individuals unless the intelligence services can prove that they are directly involved in activities posing a grave threat to national security. Additionally, democratic societies apply special controls for collecting information about members of certain professions. Notably, some states require their intelligence services to get the consent of the speaker of parliament before investigating parliamentarians.

Democratic societies restrict the collection of information from certain professions in order to protect the services they provide to the population. For example, lawyers help detainees to exercise their rights to liberty and a fair trial. If intelligence services monitor communications passed between lawyers and detainees they will violate a detainee's right to confidential access to a lawyer. Journalists provide another example. They investigate issues of interest to the public and rely on confidential communications to develop their stories. This role is essential for overseeing the activities of government agencies and uncovering wrongdoing. If intelligence services monitor journalists' communications they may jeopardise the valuable work of the media.

How does a democratic society control the use of special powers?

States legislate to give intelligence services special powers to collect information about threats to national security. Special powers are measures that are not lawfully available to other government agencies (with the exception of some police bodies) or members of the population (see page 17).

Democratic societies define and restrict intelligence services' use of special powers through legislation and regulations that outline:

- Who they are and are not permitted to investigate;
- What information they are and are not permitted to collect;
- What measures they are permitted to use to collect information;
- When they are and are not permitted to use these special powers; and
- How long they are permitted to use them for.

Democratic societies control intelligence services' use of special powers through organisations and processes created for authorising, overseeing and evaluating uses of special powers.

Who authorises the use of special powers?

In democratic societies the use of special powers is the exception rather than the rule. Democratic societies impose strict controls on the use of such powers in order to minimise the risks that accompany their use. For this reason, each time intelligence services want to use their

special powers they require the authorisation of a designated external body (see Box 3 for details of this process in Canada). Intelligence services submit a request to the designated body, justifying their need to use a specific special power. The authorising body will then make sure their specific request complies with the law.

Usually, a member of the executive, such as the minister responsible for intelligence services, or a court is responsible for authorising the use of special powers. However, the court is likely to be designated as the oversight body for cases involving significant intrusions into the lives of individuals, such as search and seizure of property and the monitoring of communications. Courts are fully independent from both the intelligence services and the executive and are in a good position to objectively analyse the requests to use special powers.

Some states require both the executive and the judiciary to authorise intelligence services' use of special powers (see for example, the Canadian model outlined in Box 3). This approach provides an additional check for ensuring that uses of special power are legal, necessary and worth pursuing given the risks involved.

How does the state authorise the use of special powers?

The process for authorising the use of special powers differs between states and often depends on the specific power intelligence services want to use. However, laws normally require that the following three steps are taken before intelligence services can use special powers (see Box 3).

First, a designated member of the intelligence services writes a request to use a specific power which normally includes:

- a description of the activity and the specific individuals and/or groups the intelligence services want to investigate;
- an explanation of the efforts intelligence services have already made to collect information and what those efforts achieved;
- the special method they want to use and exactly what they will do such as monitor calls on a specific phone line; and
- a justification addressing why the use of the special power is necessary and beneficial for the investigation.

Second, the authorising body examines the request and assesses whether:

- the proposed use of special powers complies with all relevant laws;
- the use is necessary and beneficial; and
- the use is proportionate to the level of threat posed by the activity under investigation.

Third, the authorising body issues a warrant outlining the specific measures it authorises and how long those measures may be used.

The request and authorisation process described above is documented so intelligence services and oversight bodies may later evaluate the decisions taken.

How do democratic societies oversee the use of special powers?

In democratic societies the executive and/or a designated oversight body oversee intelligence services' use of special powers by monitoring ongoing operations and reviewing completed operations.

Intelligence services provide regular reporting to the executive and/or designated oversight body on their progress during the operation. They provide summaries of information collected, progress made, and problems they have encountered. This reporting allows overseers to assess whether the use of special powers is both legal and necessary for the intelligence services to fulfil their mandate. The executive and/or a designated oversight body may terminate the use of a special power if intelligence services have failed to comply with one or all legal controls on the use of a special power, or if an oversight body determines it is no longer needed.

Finally, oversight bodies conduct reviews of the use of special powers once they are completed. In some states, oversight bodies can order intelligence services to delete information collected in illegal ways. External oversight bodies also review uses of special powers to identify trends that may help the government and the intelligence services address specific problems.

Box 3: The process for authorising the use of special powers by the Canadian Security Intelligence Service[6]

The Canadian Security Intelligence Service Act outlines the steps for the application and issuing of warrants for the intelligence services to use special powers. Any application to use special powers must be approved by both the executive and a judge.

Application for warrant

Section 21.

1. Where the Director or any employee designated by the Minister for the purpose believes, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate a threat to the security of Canada or to perform its duties and functions under section 16, the Director or employee may, after having obtained the approval of the Minister, make an application in accordance with subsection (2) to a judge for a warrant under this section.

Matters to be specified in application for warrant

2. An application to a judge under subsection (1) shall be made in writing and be accompanied by an affidavit of the applicant deposing to the following matters, namely,

   a. the facts relied on to justify the belief, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate a threat to the security of Canada or to perform its duties and functions under section 16;

   b. that other investigative procedures have been tried and have failed or why it appears that they are unlikely to succeed, that the urgency of the matter is such that it would be impractical to carry out the investigation using only other investigative procedures or that without a warrant under this section it is likely that information of importance with respect to the threat to the security of Canada or the performance of the duties and functions under section 16 referred to in paragraph (a) would not be obtained;

   c. the type of communication proposed to be intercepted, the type of information, records, documents or things proposed to be obtained and the powers referred to in paragraphs (3)(a) to (c) proposed to be exercised for that purpose;

   d. the identity of the person, if known, whose communication is proposed to be intercepted or who has possession of the information, record, document or thing proposed to be obtained;

   e. the persons or classes of persons to whom the warrant is proposed to be directed;

   f. a general description of the place where the warrant is proposed to be executed, if a general description of that place can be given;

   g. the period, not exceeding sixty days or one year, as the case may be, for which the warrant is requested to be in force that is applicable by virtue of subsection (5); and

   h. any previous application made in relation to a person identified in the affidavit pursuant to paragraph (d), the date on which the application was made, the name of the judge to whom each application was made and the decision of the judge thereon.

Issuance of warrant

3. Notwithstanding any other law but subject to the Statistics Act, where the judge to whom an application under subsection (1) is made is satisfied of the matters referred to in paragraphs (2) (a) and (b) set out in the affidavit accompanying the application, the judge may issue a warrant authorizing the persons to whom it is directed to intercept any communication or obtain any information, record, document or thing and, for that purpose,

a. to enter any place or open or obtain access to any thing;
b. to search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing; or
c. to install, maintain or remove any thing.

Matters to be specified in warrant

4. There shall be specified in a warrant issued under subsection (3)

a. the type of communication authorized to be intercepted, the type of information, records, documents or things authorized to be obtained and the powers referred to in paragraphs (3)(a) to (c) authorized to be exercised for that purpose;

b. the identity of the person, if known, whose communication is to be intercepted or who has possession of the information, record, document or thing to be obtained;

c. the persons or classes of persons to whom the warrant is directed;

d. a general description of the place where the warrant may be executed, if a general description of that place can be given;

e. the period for which the warrant is in force; and

f. such terms and conditions as the judge considers advisable in the public interest.

Use and management of personal data

What is personal data?

Personal data is information about a given individual. This includes facts such as a person's contact details, date of birth, and passport and social security numbers. Personal data also includes more detailed information about a person's private life, such as their health and employment records, religious beliefs or political opinions, details of memberships of political parties and trade unions, and details about their relationships with partners and friends. Intelligence services may need to collect personal data on individuals to identify possible threats to national security.

How do intelligence services acquire personal data?

Intelligence services acquire personal data in five main ways. First, intelligence services collect personal data from public or open sources. Second, they acquire personal data through the use of special powers, such as secretly monitoring communications (see page 17). Third, they may request information and personal data about a specific individual from domestic governmental agencies such as immigration services. Fourth, informants may provide personal data to intelligence services. Finally, intelligence services may acquire personal data about specific individuals from foreign governments and/or their intelligence services.

How do intelligence services and their governments use personal data?

Intelligence services retain much of the personal data they collect in electronic or paper files for easy access. First, they use these files to support ongoing and future investigations of threats to national security. They may also use personal data to assess individuals applying for government security clearance.

Second, intelligence services share personal data with government agencies and officials such as law enforcement authorities and prosecutors. Governments are increasingly using personal data from intelligence services to support taking legal actions against specific individuals. They use personal data in counter-terrorism operations to justify banning travel, denying visas, seizing assets and restricting an individual's movements and communications with others.

In exceptional circumstances, intelligence services are also allowed to share personal data with foreign governments and their agencies. For more information please refer to the International Intelligence Cooperation section of this guidebook.

Why do democratic societies restrict the use of personal data?

Democratic societies restrict the use of personal data by intelligence services for three main reasons. First, democratic societies restrict the use of personal data because of the inherent risks the disclosure of personal data may pose to individuals. Personal data includes information about the most private aspects of a person's life, including their medical records, religious beliefs, political opinions and personal relationships. Disclosure of such information may jeopardise their employment prospects, personal and professional relationships and personal safety.

Second, there is the potential risk that intelligence services and/or others who may have legal access to an individual's personal data will use it for illegal purposes. For example, intelligence services and/or the executive may be tempted to use personal data to discredit or blackmail political opponents. Therefore democratic governments need to restrict uses of personal data through legislation.

Finally, individuals do not normally know what personal data an intelligence services holds about them. Consequently, they may not be able to challenge the intelligence services' use of their personal data or the accuracy of the data. Therefore, it is essential that laws set clear rules for using personal data, and that oversight bodies monitor compliance with these rules.

What legal controls apply to the use of personal data?

Intelligence services need to collect and make use of certain personal data in order to perform their functions. In particular, they need to be able to identify particular individuals and collect information on their behaviour and activities in order to identify possible threats to national security. With this in mind, states adopt laws permitting intelligence services to use certain personal data without the consent of the individuals concerned. Through legislation they also apply strict controls to regulate the use of personal data. (See Box 4 for an example of legislation on the use of personal data by intelligence services in Germany). These controls are complex; the following discusses just three types of legal controls.

First, national laws control what types of personal data intelligence services may use. For example, laws permit intelligence services to use personal data of individuals involved in activities which threaten national security, such as their membership of a terrorist organisation. Laws require that the use of personal data is linked to a person's behaviour; that is, their involvement in activities that threaten national security. Democratic societies prohibit intelligence services from using personal data on the basis of characteristics such as a person's ethnicity, religion, or gender. In addition, laws prohibit intelligence services from using parts of an individual's data that are not linked to a national security threat, such as their medical records, even if they are involved in activities that threaten national security.

Second, laws place limits on retaining personal data. Intelligence services can only retain personal data if it is necessary for identifying and analysing a specific threat to national security. Laws require intelligence services to check their files regularly in order to update personal data files. In many democratic societies national law requires intelligence services to delete personal data that is no longer relevant or necessary, such as personal data of individuals who pose no threat to national security.

Third, the law controls access to personal data held by intelligence services. Only certain employees of intelligence services may access personal data files. The law also requires them to document all access of personal data files by these individuals. These controls aim to prevent the misuse of personal data.

Fourth, the law restricts intelligence services' release of personal data for use by other government agencies. They may only share personal data with authorised government bodies which need the information to carry out their mandates. Strict limitations are placed on the way such bodies can use personal data shared with them by intelligence services.

Who oversees the use of personal data and what do they do?

External oversight bodies oversee intelligence services' use of personal data to ensure they use data in accordance with the law. Such bodies include parliamentary and expert oversight bodies, as well as data protection institutions (see pages 34-42).

These oversight bodies scrutinise intelligence services' decisions to retain personal data and create files on certain individuals. In some states an oversight body must give intelligence services its consent before creating a file on an individual.

Oversight bodies also check the files of intelligence services to make sure they are

Box 4: Regulations on the use of personal data by the German Federal Office for the Protection of the Constitution [7]

German law imposes strict controls on the use of personal data by the Federal Office for the Protection of the Constitution (Germany's domestic intelligence service). The following extracts from two German laws are examples of good practice on the collection, retention and deletion of personal data. In Germany, all of these activities are monitored by the G10 Commission, an independent oversight body which has access to all information held by the intelligence services.

Permissible grounds for using personal data

- To fulfill its tasks, the Federal Office for the Protection of the Constitution may store, modify and use personal data if:
  1. there are actual indications of efforts or activities pursuant to section 3, subsection 1 (these activities include: efforts directed against the free democratic basic order, the existence or the security of the Federation or one of its States, or aimed at unlawfully hampering constitutional bodies of the Federation or one of its States in the performance of their duties)
  2. this is necessary for the investigation and analysis of efforts or activities pursuant to section 3, subsection 1 or
  3. the Federal Office for the Protection of the Constitution takes action under section 3, subsection 2. (that is, against activities threatening security or intelligence activities carried out on behalf of a foreign power)

Regulations on the storage, correction and erasure of personal data held by the Federal Office for the Protection of the Constitution

- The Federal Office for the Protection of the Constitution shall restrict the duration of storage (of personal data) to the extent necessary to fulfill its tasks.
- Incorrect personal data stored in files shall be corrected by the Federal Office for the Protection of the Constitution.
- When dealing with particular cases, the Federal Office for the Protection of the Constitution shall check within given periods, after five years at the latest, if stored personal data must be corrected or erased.
- Personal data stored in files shall be erased by the Federal Office for the Protection of the Constitution if their storage was inadmissible or knowledge of them is no longer required for the fulfillment of its tasks. The data shall not be erased if there is reason to believe that erasure would impair legitimate interests of the data subject. In this case the data shall be blocked and shall only be transferred with the data subject›s consent.

Oversight

- The (G10) Commission's supervisory powers shall extend to the entire scope of collection, processing and use of the personal data obtained pursuant to this Act by intelligence services of the Federation.

processing personal data in accordance with laws and regulations. They may check files on their own initiative or respond to individuals' enquiries about their files. In some states, the law requires intelligence services at times to inform oversight bodies when they share personal data with other institutions or when they delete information from their data files. Finally, in many states, oversight bodies scrutinise intelligence services' handling of requests made by individuals to access their personal data held by intelligence services (see Box 5).

Can individuals access their personal data?

In democratic states, members of the public have the right to apply to access their personal data held by intelligence services. (See Box 5 for an example of how this process works in Germany). To gain access to their personal data they submit a request directly to the intelligence services or through the member of the executive responsible for intelligence services. After viewing their personal data, they may be able to submit requests to delete and/or change data.

Box 5: German law on access to personal data held by intelligence services[8]

German law gives people a general right to access their personal data held by the intelligence services. Applications are submitted directly to the intelligence services. The following extracts illustrate how this process works.

Applying to access personal data held by the intelligence services

- The Federal Office for the Protection of the Constitution shall provide the data subject, at his/her request, with information free of charge on personal data stored on him/her, if he/she refers to concrete matters and proves to have a special interest in the information which he/she has asked for.

Grounds for refusing access to personal data

- The information shall not be provided if:
  1. this would prejudice the proper fulfillment of tasks,
  2. this could expose sources, or if it is to be feared that the Federal Office for the Protection of the Constitution›s knowledge or its modus operandi might be explored,
  3. this would impair public safety or otherwise be detrimental to the Federation or a Federal State, or if
  4. the data or the fact that they are being stored must be kept secret in accordance with a legal provision or by virtue of their nature, in particular on account of an overriding justified interest of a third party.
- The decision shall be made by the head of the Federal Office for the Protection of the Constitution or by a staff member explicitly authorised by him.
- The obligation to provide information shall not include information on the origin of the data and the recipients of the data transferred.
- Reasons for the refusal to provide information need not be given if this jeopardised the purpose being pursued by refusing to provide the information. The reasons for the refusal shall be taken on record.

Right to appeal

- In case of a refusal to provide information the data subject shall be informed of the legal basis for a reason not being given and of the fact that he/she may appeal to the Federal Commissioner for Data Protection, who shall, at his request, be supplied with the information unless the Federal Ministry of the Interior determines in a particular case that this would jeopardise the security of the Federation or a Federal State.

In some cases laws and regulations permit intelligence services to refuse requests from individuals to access their personal data. For example, they may deny requests in order to keep an ongoing investigation out of the public domain, to ensure public safety or to protect national security interests. Intelligence services do not usually have to give individuals reasons for denying their requests. However, external oversight bodies may scrutinise intelligence services' decisions to deny requests. Individuals may be able to appeal to such bodies to review their case. This helps to ensure that decisions to deny access to personal data are strictly necessary.

International intelligence cooperation

What is international intelligence cooperation?

The term "international intelligence cooperation" describes the ways in which intelligence and security services of two or more countries work together. Intelligence services cooperate with foreign entities in three main ways. First, and most commonly, intelligence services share information with their foreign counterparts. They may share and/or exchange raw data or provide analyses of information to foreign intelligence services.

Second, some intelligence services conduct joint operations with their foreign partners. For example, agents from different intelligence services may collaborate to collect information. Or intelligence services of one country may share their intelligence infrastructure with foreign intelligence services.

Third, international intelligence cooperation may involve the sharing of knowledge and expertise. For example, intelligence services may train foreign counterparts or send intelligence officers to support the work of foreign intelligence services.

Why do intelligence services cooperate with foreign governments and intelligence services?

Intelligence services cooperate with foreign partners mainly because this collaboration gives them greater access to information and expertise. Intelligence services in one country may not have enough resources or expertise to collect information about relevant threats existing in all regions of the world. Thus, they need to rely on foreign agencies; these partners have the geographical position and knowledge of specific groups, languages and cultures to collect the needed information. Intelligence services in one country may provide information to a foreign counterpart agency in exchange for information or other resources, such as equipment or money. International cooperation between intelligence services has become increasingly important because groups threatening the security of states and their populations often operate across borders and in a number of states.

What are the risks of intelligence cooperation?

Cooperation among foreign governments and intelligence services presents a variety of risks for all concerned parties. First, international cooperation poses significant risks to human rights protected under international law. Intelligence cooperation poses a particular threat to human rights when intelligence services share personal data with foreign entities. For example, an intelligence service that has received the personal data may end up using it in a way that violates human rights. They may use the personal data to identify individuals and detain them unlawfully and/or mistreat them. Generally, intelligence services tell a foreign partner how the personal data they share can be used, but ultimately they have little control over its use.

Second, in many cases intelligence services do not know how foreign bodies collect information or whether information was obtained legally. Specifically, they may not know whether a foreign body used torture or other unlawful tactics to obtain the information. However, if intelligence officials know that information obtained from foreign or domestic sources involved violating human rights, they can be considered complicit.

Third, some intelligence services may wish to cooperate with foreign partners in order to prevent their authorities from controlling their activities. Specifically they may want to avoid the legal controls and oversight their authorities may use to hold them accountable for respecting human rights while using their special powers for collecting information.

Finally, in addition to threats posed to human rights, international intelligence cooperation may damage a state's reputation and foreign relations. For example, intelligence services may cooperate with a foreign intelligence agency in ways that interfere with their state's foreign policy. Given this risk, states try to control their intelligence services' international cooperation as much as possible.

How do states control international intelligence cooperation?

National laws regulate intelligence cooperation with foreign governments and intelligence services. Such laws and regulations specify who the intelligence services may cooperate with; what rationale and conditions must exist to cooperate with those bodies; and how the government will authorise and oversee such cooperation (see Box 6 on how international intelligence cooperation is regulated in Croatia).

In view of the risks associated with international intelligence cooperation, national laws require intelligence services to obtain approval from the executive before entering into an agreement with a foreign body. In addition, the executive must usually approve joint operations or activities involving the sharing and exchange of information posing risks. Executive approval of international intelligence cooperation, especially sensitive activities, ensures that intelligence services do not operate unchecked by the state.

What controls apply to the sharing of information with foreign intelligence services?

Democratic societies have laws and regulations to control intelligence services' information sharing with foreign intelligence services (see Box 6). Laws restrict when and under what circumstances intelligence services may share information with foreign bodies. For example, intelligence services will only ask for information from foreign bodies if the information is necessary to fulfil their mandate. Likewise, they will not give information to foreign bodies unless the information is necessary for them to fulfil their mandate.

In addition, the law requires intelligence services to consider whether or not sharing of specific information will be in the best interests of the state. For example, some laws require intelligence services to consider whether sharing information with a foreign entity would serve the state's foreign policy. More importantly, intelligence services are required to consider the effects sharing of information may have on the individuals who are the subjects of the information. In democratic societies laws prohibit sharing information with foreign bodies if the information is likely to endanger the lives of individuals or lead to other human rights violations.

In addition to the laws and regulations governing intelligence work, intelligence services have their own conditions for sharing information with foreign partners. The most common examples are the principles of "originator control" and "third party rule". These informal rules apply to most international intelligence sharing. "Originator control" refers to the principle that the intelligence body giving the information dictates the limits to the use of the information. "Third party rule" means the recipient of the information is not allowed to share the information with another agency or other third party without the permission of the intelligence services that originally provided the information. These principles help to prevent unauthorised disclosure of sensitive information.

Intelligence services also attach notes to shared information that are often referred to as "caveats". These notes outline how the shared information may be used. For example, they may prohibit a foreign agency from using particular information as the basis to arrest and detain someone. Intelligence services retain the right to ask the foreign body to whom they have given information how the information has been used. Such informal rules help to minimise the misuse of information by foreign bodies and may promote more respect for human rights.

How is international intelligence cooperation overseen?

In democratic societies, external oversight bodies monitor international intelligence cooperation to ensure that it complies with the law. They monitor intelligence cooperation in several ways. First, they examine intelligence services' agreements with foreign partners to ensure agreements comply with the law.

Box 6: Croatian regulations on intelligence cooperation with foreign entities[9]

The Act on the Security Intelligence System of the Republic of Croatia provides the legal basis for the Croatian intelligence services to cooperate with foreign entities, and outlines the controls that apply to sharing personal data with foreign entities.

Article 59

1. Based on their international commitments, the security intelligence agencies may cooperate with foreign security, intelligence and other corresponding services, through the exchange of information, equipment, through jointly conducted activities from their respective scopes, and through education of employees.
2. The establishment and the suspension of the cooperation with each foreign service are approved by the National Security Council on the basis of the recommendations of the directors of the security intelligence agencies and the previously obtained opinion of the Council for the Coordination of Security Intelligence Agencies.

Article 60

1. Security intelligence agencies may communicate to the appropriate foreign services the information on the citizens of the Republic of Croatia if they have been provided with relevant data indicating that such person is a threat to the national security of the state to which data is supplied, or to values protected by the international law. The information will not be provided if that would be contrary to the interests of the Republic of Croatia or if the protection of the interests of the person concerned is of greater value.
3. The delivered data must be entered into the records. Such data shall be accompanied by a notice indicating that they may only be used for the purpose they were provided for, and that the security intelligence agency providing the data retains its right to request feedback on how the provided information has been used.

Second, in some states intelligence services must inform an oversight body about transfers of information to foreign bodies. By knowing about transfers of information over time, an oversight body is able to monitor patterns and, if necessary, question particular cooperative relationships and activities of particular intelligence services. Oversight bodies may also examine the information intelligence services have sent to foreign bodies. Seeing the shared information enables them to question whether the decision to send information was necessary and appropriate in view of the possible implications for the human rights of the individuals concerned.

Third, external oversight bodies investigate allegations of wrongdoing linked to international intelligence cooperation. For example, they conduct inquiries into the actions of intelligence services in particular cases where individuals may have been mistreated.

The intelligence services' use of powers of arrest and detention

Should intelligence services have powers to arrest and detain individuals?

In most democratic societies national law does not allow intelligence services to use powers of arrest and detention. These powers usually support law enforcement rather than the intelligence services' information gathering role. International human rights law does not permit the arrest and/or detention of individuals for the purpose of collecting information.

However, some democratic states give intelligence services a mandate to arrest and detain individuals who have committed or are about to commit criminal offences threatening national security. For example, they may arrest persons involved in the preparation of terrorist attacks or the proliferation of weapons of

mass destruction. It is most common for an intelligence service to have a mandate to use powers of arrest and detention in states that do not have a separate intelligence organisation, and to attach intelligence functions to the police. Under such systems, individuals who are responsible for intelligence collection are likely to do criminal investigations of terrorist acts and would be responsible for arresting and detaining individuals suspected of those crimes. In this context national law may need to authorise intelligence services to use powers of arrest and detention.

What international standards apply to the use of powers of arrest and detention?

Democratic societies allowing intelligence officers to arrest and detain individuals incorporate into national law the internationally accepted standards related to arrest and detention (see Box 7).

These standards are applicable to intelligence services in the following categories:

the laws and rationale for arresting and detaining individuals; the treatment of individuals in detention; and the oversight and review of arrests and detention.

Laws

Intelligence services are prohibited by law from arresting and detaining people for the sole purpose of collecting information. The law, under special circumstances, may authorise them to 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 who they have arrested and detained. There are actions they must take and actions they must refrain from taking. For example, intelligence services must ensure that a detained individual has access to a lawyer and is able to contact his or her family. Also, they must ensure a detainee has adequate living conditions while they are in detention. Intelligence services must refrain from any forms of mistreatment of detainees.

Oversight

Judicial oversight of detention is essential for preventing individuals from being detained arbitrarily. This oversight requires a court to review the legality of all detentions. The court, not the intelligence officer who arrested and detained individuals, determines whether there are legitimate grounds for ongoing detention. If detainees are not charged with a criminal offence they must be released. In addition, ombudsmen institutions or human rights monitoring bodies conduct inspections of detention facilities. In many states, such bodies may make unannounced visits to ensure that detainees are being treated correctly.

Do intelligence services need their own detention facilities?

Democratic societies do not permit intelligence services to have their own detention facilities. In states that give the powers of arrest and detention to intelligence services, these organisations share the same detention facilities used by law enforcement agencies. Common detention facilities help to ensure that intelligence officers do not detain individuals arbitrarily and treat them in accordance with national laws which recognise internationally accepted standards on the treatment of persons in detention.

The use of lethal force by intelligence services

Are intelligence services permitted to kill?

Intelligence services are not permitted to kill. International law prohibits states from killing any person except in three situations and then only under specific controls and restrictions: (1) In an armed conflict, a combatant may kill an enemy combatant, but only if a set of clearly defined conditions are met. (2) Law enforcement authorities may use lethal force if it is strictly necessary to prevent an imminent threat to life, and there is no other means for countering the threat. (3) Following judicial process, a court may impose the death penalty as a form of capital punishment for specific, serious criminal offences.

Box 7: International standards on arrest and detention

International law regulates arrest and detention by all state institutions, including intelligence services. International human rights treaties, including the International Covenant on Civil and Political Rights (ICCPR) and the Convention Against Torture (CAT), contain a number of key provisions in this regard. The UN Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment (UN Principles on Detention) supplements the rules contained in these treaties.[10] While most democratic states do not permit their intelligence services to arrest or detain anyone, if intelligence services are given these powers they are required to comply with the following international standards.

Legal basis for arrest and detention

- Everyone has the right to liberty and security of person. No one shall be subjected to arbitrary arrest or detention. No one shall be deprived of his liberty except on such grounds and in accordance with such procedure as are established by law. (ICCPR, article 9.1)

Procedural standards for arrest and detention

- Arrest, detention or imprisonment shall only be carried out strictly in accordance with the provisions of the law and by competent officials or persons authorized for that purpose. (UN Principles on Detention, principle 2)
- Anyone who is arrested shall be informed, at the time of arrest, of the reasons for his arrest and shall be promptly informed of any charges against him. (ICCPR, article 9.2)
- There shall be duly recorded:
  a. The reasons for the arrest;
  b. The time of the arrest and the taking of the arrested person to a place of custody as well as that of his first appearance before a judicial or other authority;
  c. The identity of the law enforcement officials concerned;
  d. Precise information concerning the place of custody.
- Such records shall be communicated to the detained person, or his counsel, if any, in the form prescribed by law. (UN Principles on Detention, principle 12)
- The duration of any interrogation of a detained or imprisoned person and of the intervals between interrogations as well as the identity of the officials who conducted the interrogations and other persons present shall be recorded and certified in such form as may be prescribed by law. (UN Principles on Detention, principle 23.1)
- A detained person shall be entitled to have the assistance of a legal counsel. He shall be informed of his right by the competent authority promptly after arrest and shall be provided with reasonable facilities for exercising it. (UN Principles on Detention, principle 17.1)
- Promptly after arrest and after each transfer from one place of detention or imprisonment to another, a detained or imprisoned person shall be entitled to notify or to require the competent authority to notify members of his family or other appropriate persons of his choice of his arrest, detention or imprisonment or of the transfer and of the place where he is kept in custody. (UN Principles on Detention, principle 16.1)

Standards for the protection of persons in detention

- All persons deprived of their liberty shall be treated with humanity and with respect for the inherent dignity of the human person. (ICCPR, article 10)
- No person under any form of detention or imprisonment shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment. No circumstance whatever may be invoked as a justification for torture or other cruel, inhuman or degrading treatment or punishment. (UN Principles on Detention, principle 6; ICCPR article 7, CAT article 2.2-3)
- It shall be prohibited to take undue advantage of the situation of a detained or imprisoned person for the purpose of compelling him to confess, to incriminate himself otherwise or to testify against any other person. (UN Principles on Detention, principle 21.1)
- No detained person while being interrogated shall be subject to violence, threats or methods of interrogation which impair his capacity of decision or his judgement. (UN Principles on Detention, principle 21.2)
- States shall keep under systematic review interrogation rules, instructions, methods and practices as well as arrangements for the custody and treatment of persons subjected to any form of arrest, detention or imprisonment in any territory under its jurisdiction, with a view to preventing any cases of torture. (CAT, article 11)

Oversight and review of detention

- Any form of detention or imprisonment and all measures affecting the human rights of a person under any form of detention or imprisonment shall be ordered by, or be subject to the effective control of, a judicial or other authority. (UN Principles on Detention, principle 4)
- Anyone who is deprived of his liberty by arrest or detention shall be entitled to take proceedings before a court, in order that that court may decide without delay on the lawfulness of his detention and order his release if the detention is not lawful. (ICCPR, article 9.4)
- Anyone who has been the victim of unlawful arrest or detention shall have an enforceable right to compensation. (ICCPR, article 9.5)
- States shall ensure that any individual who alleges he has been subjected to torture [..] has the right to complain to, and to have his case promptly and impartially examined by, its competent authorities. (CAT, articles 12-13)
- In order to supervise the strict observance of relevant laws and regulations, places of detention shall be visited regularly by qualified and experienced persons appointed by, and responsible to, a competent authority distinct from the authority directly in charge of the administration of the place of detention or imprisonment. (UN Principles on Detention, principle 29 .1)

Most democratic states do not permit their intelligence officers to use force of any kind. In fact, intelligence officers are subject to the same rules on the use of force as members of the public. Intelligence services must seek the assistance of the police if the use of force is required. Notably, intelligence services may call upon the police to arrest an individual who has committed or is about to commit a serious criminal offence. Additionally, intelligence officers may request that they are accompanied by the police on missions where their physical security may be threatened. For example, intelligence officers may be accompanied by a police officer to execute a warrant to remove an object or install a listening device in a private house.

Some democratic states allow intelligence services to use powers of arrest and detention (see page 27). If, while performing an arrest, intelligence officers are faced with an imminent threat to their life or the life of others they may use lethal force. In such cases, they must comply with the same laws and regulations that apply to the use of force by law enforcement agencies (see Box 8). This means that any use of force must

be strictly necessary and proportionate to the threat. Additionally, intelligence services, like law enforcement agencies, must report all use of lethal force and will be subject to an investigation by an independent body.

The control and oversight of intelligence services

Why do democratic societies control their intelligence services?

There are four main reasons why democratic societies control their intelligence services.

First, democratic societies hold elected leaders accountable for the work of all government agencies and bodies funded by public money. The intelligence services are no exception to this rule. Society must have control over intelligence services in order to account for public money used to employ staff and fund their activities.

Second, intelligence services have special powers for collecting information that are not available to other members of the society. These powers create the potential for violating human rights. Therefore, a democratic society controls intelligence services in order to protect the human rights of all individuals who come into contact with intelligence services.

Box 8: International standards on the use of force by public officials

The following extracts from the ICCPR, the UN Code of Conduct for Law Enforcement Officials, and the UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials apply to intelligence services whenever they use force against a person[11]. If states give their intelligence services powers to arrest and detain, they should ensure that they conform to these standards, as well as all other applicable international and domestic law.

- Every human being has the inherent right to life. This right shall be protected by law. No one shall be arbitrarily deprived of his life (ICCPR, article 6.1)
- Law enforcement officials may use force only when strictly necessary and to the extent required for the performance of their duty (CoC Law Enforcement Officials, principle 3)
- Law enforcement officials shall not use firearms against persons except in self-defence or defence of others against the imminent threat of death or serious injury, to prevent the perpetration of a particularly serious crime involving grave threat to life, to arrest a person presenting such a danger and resisting their authority, or to prevent his or her escape, and only when less extreme means are insufficient to achieve these objectives. In any event, intentional lethal use of firearms may only be made when strictly unavoidable in order to protect life. (Principles on the Use of Force and Firearms, principle 9)
- Whenever the lawful use of force and firearms is unavoidable, law enforcement officials shall:
  a. Exercise restraint in such use and act in proportion to the seriousness of the offence and the legitimate objective to be achieved;
  b. Minimize damage and injury, and respect and preserve human life; (Principles on the Use of Force and Firearms, principle 11)
- Governments shall ensure that arbitrary or abusive use of force and firearms by law enforcement officials is punished as a criminal offence under their law. (Principles on the Use of Force and Firearms, principle 7)
- Governments and law enforcement agencies shall ensure that an effective review process is available and that independent administrative or prosecutorial authorities are in a position to exercise jurisdiction in appropriate circumstances. (Principles on the Use of Force and Firearms, principle 22)
- Persons affected by the use of force and firearms or their legal representatives shall have access to an independent process, including a judicial process. (Principles on the Use of Force and Firearms, principle 23)

Third, their information gathering role has potential for disrupting political parties, media and other institutions and professions. The state needs to control intelligence services to protect such vital components of a democratic society.

Fourth, democratic societies need control over intelligence services because the law allows them to operate secretly. For example, they may secretly listen to an individual's communications or film and photograph their private homes. The individual may be unaware that intelligence services are taking measures against them. He or she is not in a position to challenge those actions. Furthermore, individuals and the public at large are unlikely to be able to monitor intelligence services' actions that are done in secret even when they are legal. Given that intelligence services are not subject to the same level of public scrutiny as other government agencies, the potential for ineffective or illegal practices is high. Hence, governments need control over secret operations to ensure intelligence services are performing their work effectively and in compliance with the law.

Which institutions control and/or oversee intelligence services?

Five main types of institutions control and/or oversee intelligence services: the internal management of the intelligence service (pages 32-33), the executive (page 33), the judiciary (page 33), parliament (pages 34-42), and expert oversight bodies (pages 34-42).

Internal management

What role does internal management play in controlling intelligence services?

Internal management controls day-to-day intelligence activities. It ensures that intelligence officers conduct their work effectively and meet the executive's requirements. It is also responsible for the intelligence services' compliance with relevant national and international laws.

Internal management establishes procedures for assigning, reporting on and evaluating all intelligence activities. Additionally, it issues ethical codes of conduct and other guidance for intelligence staff. Internal management also coordinates the processes for evaluating the performance of staff.

To whom do intelligence services report?

Intelligence services report to the executive, parliament and the public. They report to the executive about their prospective, ongoing and completed activities. The executive uses intelligence services' reporting to evaluate whether they are fulfilling their mandate and meeting the overarching priorities for intelligence services.

Intelligence services report to parliament either directly or through the minister responsible for intelligence. Parliament uses intelligence services' reports to scrutinise intelligence activities and inform decision-making on future budget allocations for intelligence services. Intelligence services sometimes submit reports to the plenary of parliament which are usually public.

Intelligence services also report to independent intelligence oversight bodies; these reports often contain classified information. In some systems, intelligence services and/or the minister or ministers in charge report to a designated committee within parliament or an expert oversight committee that operates outside of parliament.

Intelligence services also write reports for public audiences. Public reports raise awareness of the work of intelligence services and foster public confidence. They are usually posted on the intelligence services' webpage.

National law generally requires intelligence services to report to parliament and/or the executive about their activities on a periodic basis such as every six months. Parliamentary and expert oversight bodies may request additional reports from intelligence services, or from the executive minister in charge of intelligence services, about particular issues.

Who appoints directors of intelligence services?

National laws outline the procedures for appointing directors of intelligence services and the qualifications required by directors. The head of government, or the minister responsible for

intelligence services, usually appoints directors of intelligence services. In many states, the executive must consult with leaders of opposition parties before appointing directors. They also may need to consult the parliament. Parliament may ask questions about the nominee, or in some cases, organise a hearing with him or her. The involvement of other stakeholders in the appointment of directors helps to prevent the executive from appointing persons who will protect or promote their own political interests.

Why are directors of intelligence services appointed for a fixed period?

The law requires directors of intelligence services to be appointed for a fixed term of office. They can only be removed from office if they breach specific rules. A fixed term of office helps to protect directors' jobs from political pressures or changes in government. For example, fixed terms of office make it difficult for an executive member to force his or her own agenda on intelligence services by threatening to remove a director from office if he or she does not take a particular course of action.

The executive

What role does the executive play in controlling and assessing intelligence services?

In democratic societies, the executive has overall control of intelligence services. Members of the executive establish the overarching policies and priorities for intelligence services. Additionally, the executive is politically responsible for the intelligence services; it is accountable to parliament and the public for intelligence activities.

The executive is responsible for authorising intelligence activities that pose a significant risk to the safety of individuals, the state's foreign relations and/or its reputation. In authorising these activities the executive takes political responsibility and also provides additional controls over the intelligence services.

The executive oversees intelligence services to ensure they perform their functions effectively and in accordance with the law. If there are allegations of wrongdoing made against intelligence services, the executive may initiate inquiries into particular intelligence activities.

While the activities of intelligence services are based on statutes, the executive issues regulations to help clarify and implement the laws. For example, the executive may issue guidelines on ethical standards based on statutes relating to intelligence services.

The judiciary

What is the role of the judiciary in controlling and overseeing intelligence services?

Judiciaries play an important role in controlling and overseeing intelligence services. In many states, they authorise and oversee the use of intelligence services' special powers (see pages 18-19 and Box 3). Courts also settle complaints made against the intelligence services and, if required, prescribe remedies for any wrongdoing (see pages 43-45). Through their rulings, courts set standards for controlling the future conduct of intelligence services.

Courts also adjudicate on matters concerning access to or disclosure of information relating to intelligence services. In many democratic states, individuals and civil society organisations are able to request information about any government agency. Gaining access to this information can enable society to oversee the activities of the government, including its intelligence services. Courts may be required to adjudicate on such claims concerning information about or held by intelligence services. These decisions are made on the basis of access to/freedom of information laws. Additionally, courts may be required to adjudicate on cases brought against persons accused of unlawfully disclosing classified information held by intelligence services.

Finally, in democratic states the executive may ask current or former judges to carry out judicial inquiries into past events or activities involving the intelligence services.

Parliament

What is the role of parliament in overseeing intelligence services?

1. Legislating

   Parliaments draft and adopt the laws regulating intelligence services and establish institutions to oversee them. While drafting intelligence services legislation, members of parliament try to include comprehensive provisions on external oversight and accountability, respect for the rule of law and human rights. Parliaments also scrutinise, and if necessary, amend proposed legislation. Finally, parliaments identify and amend gaps in existing legislation.

2. Controlling finances

   Parliaments also control the intelligence services' use of public money; they approve future budgets and review past spending. Each year parliaments approve projected spending. During this process they are able to question the executive about their policies and priorities for the intelligence services. Parliament has the power to reject or limit funding if the executive and/or the intelligence services refuse to address its concerns. Thus, parliamentarians use their budgetary oversight role to influence the policies and actions of intelligence services.

   In addition to approving prospective spending, parliaments are involved in reviewing past expenditures of intelligence services. In some states, parliaments have accounts committees that review all government expenditures. In other states, national audit institutions perform this function under the supervision of parliament.

3. Overseeing policies and activities

   Parliaments also oversee the administration, policies and operational activities of intelligence services. This helps to ensure they are fulfilling their mandate effectively and in accordance with the law. Parliamentary oversight of intelligence services is organised in a variety of ways. In some states, parliamentary committees for defence or the interior may be responsible for intelligence oversight. However, an increasing number of states are establishing special parliamentary committees to oversee intelligence services (see pages 38-42). Elsewhere, parliament plays a more indirect role in overseeing the intelligence services. It mandates an external, expert body to carry out the day-to-day oversight of intelligence services. Parliament may play a role in appointing the members of expert oversight bodies. In many democratic states, such bodies report to parliament, which can then take action to ensure that the expert body's findings and recommendations are addressed.

   Finally, parliaments oversee intelligence services by setting up inquiries into particular events or activities involving the intelligence services.

Expert oversight bodies

What is the role of expert intelligence oversight bodies?

An increasing number of states are establishing expert intelligence oversight bodies in addition to or instead of parliamentary oversight bodies. These bodies are independent from intelligence services, the executive and parliament. They focus exclusively on overseeing particular intelligence services. Expert oversight bodies are commonly mandated to oversee the legality of the work of intelligence services but their mandates may also include monitoring the effectiveness of operations, administrative practices, and the finances of intelligence services (see page 38 and Table 2).

Parliament usually appoints oversight bodies and they report to parliament and/or the executive. In contrast to members of parliamentary intelligence oversight committees, most members of expert oversight bodies are not members of parliament. They are normally senior public figures, including prominent members of civil society, current and former members of the judiciary and former politicians.

Table 2: A comparison of selected intelligence oversight bodies in Belgium, Canada, South Africa and the United Kingdom[12]

	Belgium	Canada	South Africa	United Kingdom
Name	Standing Intelligence Agencies Review Committee	Security Intelligence Review Committee	Joint Standing Committee on Intelligence	Intelligence and Security Committee
Type	Expert oversight body	Expert oversight body	Parliamentary oversight body	Parliamentary oversight body
Other relevant oversight bodies	Senate commission responsible for monitoring the Standing Intelligence Agencies Review Committee	Inspector General of the Canadian Security Intelligence Service (IG)	Inspector General for Intelligence (IG)	Intelligence Services Commissioner; Interception of Communications Commissioner; Investigatory Powers Tribunal
Composition	3 members; Must be at least one member from each linguistic group; Cannot hold elected office.	2-4 members; Cannot be members of parliament.	15 members of parliament	9 members of parliament drawn from both houses; Cannot be ministers (i.e. members of the executive).
Appointment of Members	Appointed by the Senate (upper house of parliament).	Appointed by the executive following consultation with the leaders of opposition parties.	Appointed by parliament through proportional representation, and on the basis of nominations by parties.	Appointed by the prime minister in consultation with the leader of the largest opposition party.
Tenure of office	5 years, renewable twice.	5 years, renewable.	Duration of parliament.	Duration of parliament.

	Belgium	Canada	South Africa	United Kingdom
Mandate	Review the activities and methods of the intelligence services, their internal rules and directives; The committee should ensure: (1) the protection of constitutional and other rights by the intelligence services; (2) the coordination and effectiveness of the intelligence services; Investigate complaints; Provide advice on draft legislation, decrees and directives.	Review the services' performance of its duties and functions; Review directions issued by director of the intelligence service; service's regulations agreements with domestic and foreign entities; reports of the service and the IG; The committee should ensure that: (1) the service's activities comply with applicable law; and (2) the service does not exercise its powers in an unreasonable or unnecessary way; Direct the service or IG to conduct reviews of specific activities; or where it considers that this would be inappropriate, conduct such a review itself; Investigate complaints.	Review finances of intelligence services, including reports of the audit office; Receive complaints and order the IG or the intelligence services to investigate them; - Review reports of the IG; Make recommendations on intelligence-related legislation and any other matter related to national security and intelligence.	To examine the expenditure, administration and policy of the intelligence services.
Investigative Powers	Can summon any person to testify under oath before the committee; Can request the assistance of law enforcement authorities to force persons to comply.	When investigating complaints, the committee has the powers of a court: it may summon and enforce the appearance of persons before the committee, and can compel them to give oral or written evidence on oath.	May require any minister, a head of an intelligence service or the IG to appear before it; Right to hold hearings and subpoena witnesses.	May call on ministers and other relevant officials to testify.

	Belgium	Canada	South Africa	United Kingdom
Access to classified information	Access to all information they deem necessary; Intelligence services must, on their own initiative, supply the committee with all internal rules & directives.	Unlimited access to all information necessary for the performance of its duties and functions.	Some limitations on access to information held by intelligence services; the names of agents and/ or sources can be withheld from the committee.	The responsible minister can limit the committee's access to sensitive information which could reveal details of operations, or sources and methods of the intelligence services.
Triggers for investigations	Own initiative; A complaint; At request of parliament; At request of the responsible minister.	Own initiative; A complaint; A referral by the canadian human rights Commission.	Can draft a special report at the request of parliament, or the responsible minister(s).	Own initiative; At the request of the responsible minister.
Reporting	Obligatory annual report to president of both houses of parliament and the responsible minister; Special reports first presented to the responsible minister, later to the Senate (upper house). Reports to parliament do not contain any classified information.	Obligatory annual report; Reports sent first to the executive who must place the report before parliament within 15 days; Issues special reports when requested by minister or on own initiative; Obligation to consult with the director of the intelligence service before making a report public.	Obligatory annual report to parliament the president, and responsible minister(s); Reports cannot contain information that could be harmful to national security.	Obligatory annual report; may also issue reports on any relevant matter; All reports are sent first to the prime minister who then submits them to parliament; The prime minister decides what information should be removed from the public version of the report.

An in-depth study of parliamentary and expert intelligence oversight bodies

This section examines the role played by specialised parliamentary oversight committees and expert intelligence oversight bodies. It addresses questions about their mandates; powers; resources; handling of classified information; relationships with intelligence services; independence; reporting functions; and finally, the advantages and disadvantages of both parliamentary and expert oversight bodies.

Which aspects of intelligence services' work are overseen by parliamentary and/or expert oversight bodies?

Parliamentary committees and/or expert oversight bodies oversee all aspects of intelligence services (see Table 2 for examples). They focus on four areas:

1. Oversight of the legality of operations and policy

   Overseers evaluate whether existing policies and all aspects of ongoing intelligence operations comply with national law and international standards. They also assess whether completed intelligence operations and activities have met legal requirements. Finally, overseers review plans for future intelligence operations and determine whether those activities will comply with existing laws, regulations and international standards.

2. Oversight of effectiveness of operations

   Overseers monitor the effectiveness of intelligence operations. They determine whether intelligence services are effectively performing their functions, activities and tasks in accordance with the law and the executive's policies and priorities.

3. Oversight of administrative practices

   Overseers monitor intelligence services' administrative practices. They examine human resources policies and management practices among other things.

4. Oversight of financial management

   Overseers monitor intelligence services' internal financial activities including their budgeting and expenditures.

In some systems states establish only one parliamentary or expert oversight body to monitor and evaluate intelligence services' activities. However, more commonly, states engage more than one oversight body to monitor all the aspects of intelligence work. For example, a state may assign a parliamentary oversight committee the responsibility for monitoring the effectiveness of intelligence activities, and give an expert oversight body the responsibility for monitoring the legality of their activities. Regardless of the precise composition of the system of oversight, democratic states ensure that all aspects of intelligence services' activities are overseen by one or more external bodies.

What legal powers do oversight bodies have?

Democratic societies ensure that parliamentary and expert oversight bodies' roles, mandates and powers are based on legislation (see Table 2 for examples). The law requires the executive and intelligence services to cooperate with oversight bodies; this is essential for performing their role.

The law gives oversight bodies the powers needed for scrutinising the work of intelligence services, which is necessary for holding them accountable for their actions.

First, the law gives oversight bodies the power to act independently and to initiate their own investigations without the need to obtain prior permission from the executive or the intelligence services.

Second, the law gives oversight bodies full access to all information relevant for their work, including the secret files held by intelligence services. Access to this information is essential for determining whether, among other things, intelligence services are operating effectively and in compliance with the law. An intelligence officer's failure to comply with an oversight body's request for information may be considered a criminal offence under the law. In many states, an oversight body may call upon law enforcement authorities to compel individuals to comply with their requests for information.

Third, oversight bodies have the authority to call upon ministers and officials responsible for intelligence services to give answers to their questions related to intelligence work. In many states, these individuals must testify under oath to the oversight body.

Finally, oversight bodies are free to visit the premises of intelligence services. Such visits may be arranged in advance with intelligence services, or unannounced.

Why do oversight bodies need financial and human resources?

In addition to legal powers, oversight bodies require financial and human resources to carry out their role effectively. Oversight bodies need sufficient funding to hire permanent staff and to engage the services of specific experts when needed. They also need funding to buy equipment, such as computers. Given that they handle highly sensitive information, they need highly sophisticated computer equipment and technical experts to set up security systems.

Oversight bodies hire permanent staffers who perform roles that are essential to their organisation. Staffers do much of the day-to-day work of oversight bodies. Their tasks include preparing for inspections, conducting analyses of intelligence activities and reporting on the oversight body's investigations. While the members of both parliamentary and expert oversight bodies may change, staffers often remain with the organisation for longer periods than members. Thus, they are able to provide important continuity of activities as well as provide the organisation with "institutional memory". Their long tenures also give them developed knowledge and expertise in many aspects of intelligence work.

Parliamentary oversight bodies usually select staffers who are already employed by parliament. Expert oversight bodies usually hire their staff from outside of government. In both cases staffers must receive security clearances to ensure they can be trusted to handle sensitive information related to intelligence services.

Overseeing intelligence services requires expertise and knowledge of complex practices that very few people outside of the intelligence community possess. Therefore, in some cases they need to hire intelligence experts to help them do investigations and effectively deal with complex issues related to intelligence work. Likewise, they often need IT and telecommunications experts with intelligence backgrounds to help them gain a better understanding of the complex electronic techniques that are used by intelligence services.

How do overseers monitor intelligence services?

Parliamentary and expert oversight bodies use many different methods to monitor the activities of intelligence services. The methods used depend on the oversight body's mandate and legal powers.

First, they read classified and unclassified reports produced by intelligence services. Reports give them useful information relating to all aspects of intelligence work. This stimulates further questions which may lead to a better understanding of internal processes.

Second, they do random sampling of information intelligence services have processed or stored. Random sampling can be done during regular inspections or through unannounced visits. For example, if they wish to assess whether intelligence services are using personal data in accordance with the law, they randomly select a number of individual files and check to see if these samples meet the requirements.

Third, they conduct thematic investigations to carefully examine a specific area of intelligence work. These investigations usually focus on broad areas rather than specific events or activities. Oversight bodies often select themes based on particular concerns. These may have been brought to their attention by the public or governmental and non-governmental entities, often as a follow-up to previous inquiries or inspections.

Fourth, they also conduct investigations into specific events or allegations concerning intelligence services. They initiate investigations of specific incidents on their own or do them when the executive and/or parliament have inquiries. These investigations examine all relevant information held by intelligence services relating to specific events and allegations.

Finally, some parliamentary and expert oversight bodies investigate specific complaints made by individuals (see pages 43-46). By investigating specific complaints, overseers get an insight into broader problems in the work of intelligence services. Oversight bodies look for patterns in the complaints they receive; this can serve as the basis for further investigations.

How do oversight bodies report on their activities?

Generally, the law requires oversight bodies to issue annual public reports on their activities. These reports usually include information about their current membership, investigations carried out, their findings, finances, and recommendations. The recommendations advise the intelligence services and the executive on how they can improve their accountability, transparency, legality and effectiveness.

Oversight bodies may provide additional reports in a given year. They produce special reports describing investigations they have conducted on specific events or general themes. Oversight bodies usually produce two versions of their reports. They produce one version for the executive and the intelligence services which may contain classified information and a second version for the public which generally does not contain classified information. Oversight bodies consult with the executive and intelligence services before releasing public reports. This consultation gives the executive and intelligence services the chance to share any concerns they may have regarding the inclusion of sensitive information in the report.

Why are public reports important?

First, public reporting informs society about intelligence services' activities while also promoting public understanding and confidence in the intelligence oversight body.

Second, overseers use their reports to try to bring about change within the intelligence services, to executive policies on intelligence, or to the legislation that regulates intelligence activities. The reports of oversight bodies often contain recommendations on how to improve particular policies and practices. Overseers can follow up on such recommendations in subsequent years to hold the intelligence services and the executive to account for addressing problems previously identified in their organisation.

Is there a conflict between the right to know and the need to keep information secret?

In order to monitor intelligence services, parliamentary and expert oversight bodies require detailed information about their activities. In most democratic states they have a legal right to access all information relevant to their work. On the other side, intelligence services need to protect information, which, if made public, could harm ongoing investigations or expose their methods and sources used for collecting information. The public disclosure of such information could also be harmful to national security. Intelligence services are often uneasy about overseers having full access to their information because they are afraid that classified information might be leaked.

Besides, many intelligence services are concerned that overseers might undermine their confidentiality obligations regarding personal data. The law requires intelligence services and their personnel to treat personal data confidentially, and restricts the sharing of such information.

Given these competing demands on information held by intelligence services, there is a potential for conflict between intelligence services and overseers regarding access to information. However, several measures can prevent such conflicts (see below).

How can the information needs of oversight bodies and intelligence services be reconciled?

Special measures help make sure that oversight bodies handle classified information appropriately. These measures help to reassure intelligence services that overseers will not leak classified information.

First, parliamentary and expert oversight bodies hold most of their meetings in private. The content of these meetings is not made public.

Second, it is common practice in democratic states for the law to make the disclosure of classified information a criminal offence. In many states,

members of oversight bodies and their staff must obtain security clearances, before being allowed access to classified information. This means that they are screened to ensure that they are can be trusted to have access to classified information. Additionally, overseers may be required to sign special agreements stating they will not disclose classified information.

Third, oversight bodies need to take measures to prevent staff from disclosing classified information. They usually adopt policies prohibiting members and staffers from taking classified information off the premises. Also, special security measures may apply to protect electronic and hard copy documents containing sensitive information.

Finally, laws on the protection of personal data apply to oversight bodies, as they do to any other public institution. The law requires oversight bodies to keep personal data confidential. Oversight bodies may only disclose them with the consent of the person concerned, and in accordance with other specific criteria set out in law.

Why is the relationship between intelligence services and oversight bodies important?

Oversight bodies generally seek to develop a constructive relationship with the intelligence services they monitor. This is because it is very difficult for overseers to monitor intelligence services properly without their cooperation. Overseers rely on intelligence services to facilitate their access to the information needed. Oversight bodies can gain the trust of intelligence services by treating classified information with care and by keeping them informed about oversight activities.

Intelligence services benefit too from a constructive working relationship with oversight bodies. The reports of oversight bodies can foster their legitimacy and build public confidence in their work. In some cases, oversight reports can also help intelligence services to make a case for additional financial or human resources. Additionally, if allegations are made about intelligence services, an investigation by an oversight body can sometimes help re-establish public confidence in them. Oversight bodies can also play a role in protecting intelligence services against potential misuse by the executive. Intelligence officials can report inappropriate or illegal orders they receive to the oversight body. Considering these benefits, it is generally in the interest of intelligence services to cooperate with oversight bodies.

While the working relationship needs to be constructive, it should not be too close. The public will only perceive oversight bodies as independent, and therefore effective, if they maintain a certain distance from the intelligence services.

How do democratic societies ensure the independence of intelligence oversight bodies?

Parliamentary and expert oversight bodies are independent organisations. They cannot be part of the executive or the intelligence services, as they must oversee those who collect and use intelligence information.

Democratic states adopt laws giving intelligence oversight bodies an independent legal identity. The intent of these laws is to protect their organisational and operational independence. These laws authorise oversight bodies to pursue their own activities without interference from the executive or intelligence services. For example, they select the cases or themes they will investigate and decide how they will conduct investigations. The independent legal identity of oversight bodies means that they cannot take any instructions from the executive or the intelligence services.

Oversight bodies can also decide independently which information they need to access from the intelligence services. Legally guaranteed access to information ensures that neither the intelligence services nor the executive may control the work of oversight bodies by restricting their access to information. In some instances, oversight bodies may rely on the courts to require intelligence services to give them access to relevant information.

Oversight bodies can also make independent decisions related to reporting. In practice, overseers consult intelligence services and the executive before publishing a report. However, the executive and intelligence services have no legal recourse to stop oversight bodies from publishing their independent findings and

recommendations in reports.

In many democratic states, intelligence oversight bodies also have budgetary independence. This means that they can request their own funding from parliament and manage their own budgets. Because they are financially independent, other organisations (e.g. the executive, intelligence services) cannot influence their decisions by threatening them with funding cuts.

How can the independence of members of oversight bodies be ensured?

The independence of an oversight body is only guaranteed if its members and staff remain independent. This implies that they do not misuse their positions for personal gain or for advancing the interests of others. Thus, democratic societies adopt laws to make sure that individuals appointed to oversight bodies are and remain independent.

Usually, the law regulates the selection and appointment of members of oversight bodies. In many states parliament appoints members of oversight bodies. This means that overseers are chosen by an institution that is independent from those being overseen. This is necessary to ensure the independence of persons who serve on oversight bodies. In a few states, the executive is responsible for appointing members of oversight bodies but its choices need the approval of parliament and in some cases the judiciary.

The fact that members of oversight bodies are appointed for fixed terms of office gives them additional independence and protects them against external pressure. As terms of office are defined by law, politicians cannot arbitrarily dismiss them. Dismissals are only possible, if the person has committed a serious offence or failed to perform his or her duties. In some countries, the law does not allow members of oversight bodies to serve a second term. By limiting mandates to one term, legislators have sought to prevent members of oversight bodies from misusing their position with the goal of influencing decisions to re-appoint them.

As an additional measure for ensuring independence, the law may prohibit serving members of oversight bodies from holding other positions. For obvious reasons, members of oversight bodies cannot serve in intelligence services. But the law may also prohibit overseers from holding membership of a political party or engaging in commercial activities. This helps to prevent a possible conflict of interests.

What are the advantages of parliamentary oversight bodies?

Parliamentary oversight bodies have two main advantages when compared with expert ones. First, and most importantly, parliamentary oversight has more "democratic legitimacy" because it is carried out by elected individuals; those who oversee intelligence services have a direct link with the public. By contrast, members of expert oversight bodies have only an indirect legitimacy, because they are normally selected by either parliament or the executive.

Second, parliamentary oversight bodies are better placed to directly influence the policies and activities of the executive and intelligence services. Parliament has two main tools at its disposal in this regard: it may be able to pass or amend legislation on the intelligence services; it can also use its power to approve or reject budgets in order to persuade the executive and/or the intelligence services to change policies or practices. This means that the findings and recommendations of parliamentary oversight bodies can quickly influence decisions and force change on intelligence legislation and budgets. Expert oversight bodies do not have these instruments available to influence the executive and the intelligence services. In most cases, they can only issue findings and recommendations to parliament, the executive, and the intelligence services.

What are the advantages of expert oversight bodies?

In comparison to their parliamentary counterparts, expert oversight bodies offer significant advantages.

First, expert oversight bodies are usually independent from political influences while parliamentary oversight can become politicised. Members of parliamentary oversight committees are more likely to use their positions for political purposes. This is a particular problem for members of parliament

belonging to the governing party. They may be unwilling to investigate particular activities of the intelligence services that could reveal findings that are damaging or embarrassing for the executive. This stems from the desire of MPs to protect their own political party, and potentially their own political ambitions. By contrast, members of parliamentary oversight committees from opposition parties may exploit their position to attack the government. For example, they may attempt to launch investigations for the purposes of damaging the government rather than to genuinely carry out their oversight mandate. These realities inhibit parliamentary committees from fully conducting impartial oversight of intelligence services.

Second, unlike parliamentarians, members of expert oversight bodies can focus exclusively on overseeing the intelligence services. Parliamentarians serving on intelligence oversight committees focus on more than just intelligence services. For example, they take part in plenary debates, serve on other committees and spend time meeting with their constituents.

Third, members of expert oversight bodies usually remain in office for longer periods than parliamentary committee members. Longer periods in the job enable members of expert oversight bodies to develop knowledge of and expertise in the intelligence field. Members serving on parliamentary committees tend to leave more frequently and do not generally develop the same level of knowledge and expertise.

Finally, since members of expert oversight bodies are generally less likely to be influenced by politics, they are probably also less likely to leak sensitive information for political purposes. Also, there are often greater numbers of parliamentarians serving on committees who have access to classified information compared to members of expert oversight bodies. Thus, parliamentary committees are more likely to misuse sensitive information for political reasons such as leaking information to discredit political opponents. Intelligence services place much value on the security of their information. In many states intelligence services generally distrust parliament and may fear that members of parliamentary oversight committees will leak classified information.

Complaints about intelligence services

How can the public complain about intelligence services?

In democratic societies, individuals have a right to complain about any action taken against them by a public institution, including intelligence services. Any person can challenge an action that an intelligence service might have taken against them, including arrest and detention, the search of their home or the interception of their communications.

Persons who believe they have been unfairly or unlawfully treated by intelligence services file their complaints with an independent body. (See Box 9 for an example of how complaints about intelligence services can be handled). This complaints-handling body is normally a court or a non-judicial body such as an ombudsman or expert intelligence oversight body. This body must first assess whether the intelligence service took action against the person concerned and, if so, whether it used its powers in compliance with the law.

If the complaints-handling body finds a complaint to be valid, it may request or order the intelligence service to remedy the situation. Common examples of remedies include the payment of financial compensation or the deletion of information collected unlawfully. Whether or not a complaints-handling body can issue legally binding orders to the intelligence services depends on its status. Judicial bodies can issue binding orders which intelligence services must comply with. In most states, non-judicial bodies, such as expert oversight bodies and ombudsmen, can issue recommendations to intelligence services. They are not legally obliged to comply with such recommendations but the complaints-handling body may be able to report non-compliance to the executive, and could even go to the media.

Box 9: Complaints-handling by Canada's Security Intelligence Review Committee (SIRC)[13]

In addition to overseeing the activities of the Canadian Security Intelligence Service, the SIRC investigates complaints made about the intelligence service. It holds in camera hearings and has the powers of a court to summon witnesses and receive evidence under oath. The following articles from the Canadian Security Intelligence System (CSIS) Act outline this process.

Section 41.

1. Any person may make a complaint to the Review Committee with respect to any act or thing done by the (intelligence) Service and the Committee shall, subject to subsection (2), investigate the complaint if :
   a. the complainant has made a complaint to the Director with respect to that act or thing and the complainant has not received a response within such period of time as the Committee considers reasonable or is dissatisfied with the response given; and
   b. the Committee is satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith.

Section 45.

A complaint under this Part shall be made to the Review Committee in writing unless the Committee authorizes otherwise.

Section 48.

1. Every investigation of a complaint under this Part by the Review Committee shall be conducted in private.
2. In the course of an investigation of a complaint under this Part by the Review Committee, the complainant, deputy head concerned and the Director shall be given an opportunity to make representations to the Review Committee, to present evidence and to be heard personally or by counsel, but no one is entitled as of right to be present during, to have access to or to comment on representations made to the Review Committee by any other person.

Section 50.

The Review Committee has, in relation to the investigation of any complaint under this Part, power:

1. to summon and enforce the appearance of persons before the Committee and to compel them to give oral or written evidence on oath and to produce such documents and things as the Committee deems requisite to the full investigation and consideration of the complaint in the same manner and to the same extent as a superior court of record;
2. to administer oaths; and
3. to receive and accept such evidence and other information, whether on oath or by affidavit or otherwise, as the Committee sees fit, whether or not that evidence or information is or would be admissible in a court of law.

Section 52.

1. The Review Committee shall,
   a. on completion of an investigation in relation to a complaint under section 41, provide the Minister and the Director with a report containing the findings of the investigation and any recommendations that the Committee considers appropriate; and
   b. at the same time as or after a report is provided pursuant to paragraph (a), report the findings of the investigation to the complainant and may, if it thinks fit, report to the complainant any recommendations referred to in that paragraph.

Which institutions handle complaints about the intelligence services?

In most states individuals can submit complaints about intelligence services to general ombudsman or human rights institutions and/or the ordinary courts. However, an increasing number of states have established special complaint-handling mechanisms, both judicial and non-judicial, to receive complaints relating to the intelligence services (see Box 9). Specialised intelligence oversight bodies often also act as non-judicial complaints-handling mechanisms.

States usually prefer to entrust specialised institutions, rather than the regular courts, with the handling of complaints related to their intelligence services for two reasons. First, such bodies can have security-cleared staff and they have procedures in place to handle classified information on a regular basis. Second, a specialised judicial or non-judicial body can develop knowledge of intelligence issues that ordinary courts or a general ombudsman or human rights institution may not have.

It is good practice to establish an appeal procedure against the decisions of specialised complaint mechanisms. Usually, ordinary courts process such appeals.

Why do some states notify people when special powers have been used against them?

A complaints-handling process assumes that individuals are aware of measures that have been taken against them by intelligence services. This is often not the case when intelligence services use special powers secretly, such as monitoring a person's communications. If people have no knowledge of actions taken against them they cannot challenge those actions by filing a complaint. Nor do they know how such actions will affect their lives. Because individuals often cannot challenge such actions, an increasing number of democratic states require intelligence services to inform individuals about secret measures that have been used against them. This notification usually takes place after a fixed period of time and is given only when it would not jeopardise ongoing investigations or reveal the specific sources and methods used by the intelligence services (see Box 10).

Box 10: German law on notifying individuals after special powers have been used against them[14]

Many European states require their intelligence services to inform persons against whom they have used special powers. The following extract from German law shows the scope of this requirement. Notification does not take place in all cases, and may be postponed on specific grounds. In Germany, an expert oversight body (G10 Commission) oversees the intelligence services' compliance with these regulations.

- The data subject shall be informed of restrictive measures pursuant to Section 3 after their discontinuation.
- Such notification shall be withheld as long as it cannot be ruled out that informing the data subject might jeopardise the purpose of the restriction or as long as any general disadvantages to the interests of the Federation or of a Federal State are foreseeable.
- Where such notification continues to be withheld pursuant to sentence 2 twelve months after termination of the measure, its continued deferment shall require the approval of the G10 Commission. The G10 Commission shall determine the duration of the continued deferment.
- No notification shall be necessary where the G10 Commission has unanimously found that:

  1. one of the conditions stipulated in sentence 2 continues to apply five years after termination of the measure,
  2. it is practically certain that such a condition will continue to apply in the future
  3. the conditions pertaining to erasure apply both at the collecting agency and at the receiving agency.

What makes a complaints-handling body effective?

Like oversight bodies, complaints-handling bodies are independent from both the executive and the intelligence services. They need the legal power to access all information, officials and premises in order to investigate a complaint.

Complaints-handling bodies are more effective if they can issue orders that are legally binding on intelligence services. For example, this power enables them to require intelligence services to pay compensation to an individual who was wrongly treated by an intelligence officer. Similarly, they could require intelligence services to delete information which was acquired through the unlawful infringement of an individual's rights.

In order for complaints-handling bodies to be effective in investigating and remedying violations of individuals' rights, they need to be easily accessible. Members of the public must be aware that complaints-handling bodies exist and be able to file a complaint if necessary. These bodies take several measures to ensure that they are accessible. First, they advertise their role to the public and provide information on how complaints can be filed. For example, they establish websites and make leaflets available in public buildings. Second, they make sure that there is no cost to submit a complaint. Finally, they guarantee that complaints will be treated confidentially. This is essential to enable people to complain without fear of reprisals from intelligence services.

Further Reading

Born, Hans and Ian Leigh, *Making Intelligence Accountable,* (DCAF/Norwegian Parliament: Oslo, 2005). Available in the following languages: Albanian, Arabic, Bulgarian, Croatian, Dari, English, Georgian, Indonesian, Macedonian, Russian, Serbian, Pashto, Spanish, Turkish, Ukrainian.
http://www.dcaf.ch/publications/kms/details.cfm?id=18718&nav1=5

DCAF Toolkit, Legislating for the security sector, Intelligence Legislation Model – Argentina, National Intelligence Law (and associated decrees), 2001.

DCAF Toolkit, Legislating for the security sector, Intelligence Legislation Model – Canada, Canadian Security Intelligence Service Act, 1985.

DCAF Toolkit, Legislating for the security sector, Intelligence Legislation Model – The Netherlands, Intelligence and Security Services Act 2002.

DCAF Toolkit, Legislating for the security sector, Intelligence Legislation Model – Brazilian laws on the intelligence services.

Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Second Report*¸ (Ottawa: Privy Council Office, 1981).
http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/mcdonald1979-81-eng/mcdonald1979-81-eng.htm

European Commission for Democracy Through the Law, (Venice Commission), *Report on the democratic oversight of the security services,* adopted by the Venice Commission at its 71s Plenary Session, CDL-AD(2007)016 (Venice, 1-2 June 2007).
http://www.venice.coe.int/docs/2007/CDL-AD(2007)016-e.asp

International Commission of Jurists, Eminent Jurists Panel, *Assessing Damage Urging Action, Report of the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights* (Geneva: ICJ, 2009).
http://ejp.icj.org/IMG/EJP-Report.pdf

Ministerial Review Commission on Intelligence in South Africa, *Intelligence in a Constitutional Democracy,* Final Report to the Minister for Intelligence Services, (Pretoria: 2008).
http://www.ssronline.org/edocs/review_commission_final_report20080910.doc

UN High Commissioner for Human Rights, *Human Rights, Terrorism and Counter-Terrorism*, Fact sheet No. 32, July 2008.
http://www.ohchr.org/Documents/Publications/Factsheet32EN.pdf

UN Human Rights Council, *Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight,* A/HRC/14/46, 17 May 2010.
http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.46.pdf

Endnotes

1. Extracts from Sections 12-15, *Canadian Security Intelligence Service Act*, 1984; Article 1, Act on the Security Intelligence System of the Republic of Croatia, 2006; and Article 6 of The Netherlands Intelligence and Security Services Act 2002.

2. Extracts from the Constitution of the Republic of South Africa, 1996, 198 -199, 209-210.

3. International Covenant on Civil and Political Rights (ICCPR), 16 December 1966, entry into force 23 March 1976, Article 4; UN Human Rights Committee, General Comment 29, States of Emergency (article 4), U.N. Doc. CCPR/C/21/Rev.1/Add.11 (2001).

4. Geneva Conventions 1-4, 12 August 1949, entry into force 21 October 1950.

5. ICCPR, Article 4; United Nations Human Rights Committee, General Comment 29, States of Emergency (article 4); U.N. Doc. CCPR/C/21/Rev.1/Add.11 (2001). Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights, Annex, UN Doc E/CN.4/1984/4 (1984);

6. Extracts from the Canadian Security Intelligence Service Act, 1984, Section 21.

7. Extracts from Federal Act on Protection of the Constitution, 1990, Sections 10, 12, 3; and G10 Act, 2001,. Section 15.

8. Extracts from German Federal Act on the Protection of the Constitution, 1990, Section 15.

9. Extracts from the Act on the Security Intelligence System of the Republic of Croatia, 2006

10. International Covenant on Civil and Political Rights; Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment, Annex to General Assembly Resolution, A/RES/43/173, 9 December 1988; Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Adopted and opened for signature, ratification and accession by General Assembly resolution 39/46 of 10 December 1984, entry into force 26 June 1987.

11. Basic Principles on the Use of Force and Firearms by Law Enforcement Officials. Adopted by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, 27 August to 7 September 1990; Code of Conduct for Law Enforcement Officials, Adopted by General Assembly resolution 34/169 of 17 December 1979; International Covenant on Civil and Political Rights, entry into force 23 March 1976.

12. This material was drawn from UK Intelligence Services Act 1994; UK Ministry of Justice, The Governance of Britain – Constitutional Renewal, (London: HMSO, 2008); Belgium – Act Governing Review of the Police and Intelligence Services and the Coordination Unit for Threat Assessment, 1991; Canadian Security Intelligence Service Act, 1984; South Africa – Intelligence Services Oversight Act, Act 40, 1994; and the websites of the Security Intelligence Review Committee (www.sirc-csars.gc.ca), and the Belgian Standing Intelligence Agencies Review Committee (www.comiteri.be).

13. Extracts from the Canadian Security Intelligence Service Act, 1984 ; and the website of the Security Intelligence Review Committee (SIRC): www.sirc-csars.gc.ca.

14. Extracts from the G10 Act, 2001, Section 12.

مركز جنيف للرقابة الديموقراطية على القوات المسلحة
شارع المعارف ٣٤
رام الله / البيرة
الضفة الغربية
فلسطين

هاتف: ٦٢٩٧ ٢٩٥ (٢) ٩٧٢+
فاكس: ٦٢٩٥ ٢٩٥ (٢) ٩٧٢+

مركز جنيف للرقابة الديموقراطية على القوات المسلحة
مركز جيفنور – بلوك C – الطابق السادس
شارع كليمنسو
بيروت
لبنان

هاتف: ٤٠١ ٧٣٨ ١ (٠) ٩٦١+
فاكس: ٤٠٢ ٧٣٨ ١ (٠) ٩٦١+

DCAF Head Office, Geneva
By Post:
Geneva Centre for the Democratic Control of Armed Forces (DCAF)
P.O.Box 1360
CH-1211 Geneva 1
Switzerland

For Visitors:
Geneva Centre for the Democratic Control of Armed Forces (DCAF)
Rue de Chantepoulet 11
CH-1201 Geneva 1
Switzerland

Tel: +41 (0) 22 741 77 00
Fax:+41 (0) 22 741 77 05

DCAF Ramallah
Al-Maaref Street 34
Ramallah / Al-Bireh
West Bank
Palestine

Tel: +972 (2) 295 6297
Fax: +972 (2) 295 6295

DCAF Beirut
Gefinor Center - Block C - 6th Floor
Clemenceau Street
Beirut
Lebanon

Tel: +961 (0) 1 738 401
Fax: +961 (0) 1 738 402

www.dcaf.ch