Overseeing Intelligence Services

A Toolkit

Edited by Hans Born and Aidan Wills

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

Ministry of Foreign Affairs of the Netherlands

Overseeing Intelligence Services

A Toolkit

Edited by Hans Born and Aidan Wills

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

Ministry of Foreign Affairs of the Netherlands

The Geneva Centre for the Democratic Control of Armed Forces (DCAF) is an international foundation whose mission is to assist the international community in pursuing good governance and reform of the security sector. The Centre develops and promotes norms and standards, conducts tailored policy research, identifies good practices and recommendations to promote democratic security sector governance, and provides in-country advisory support and practical assistance programmes.

Published by DCAF, Geneva
11 Rue de Chantepoulet
Geneva – 1201
Switzerland
www.dcaf.ch

Designer: Alice Lake-Hammond, www.alicelakehammond.com
Language editor: Agincourt Press
Cover photograph: Hans Kouwenhoven

This publication has been made possible by the generous support of the Ministry of Foreign Affairs of the Netherlands.

ISBN: 978-92-9222-222-2

Contents

List of Tables and Boxes

DCAF Foreword

The intelligence sector represents a last frontier in democratization and security sector reform processes. As many established democracies have demonstrated, democratic governance and the rule of law reach the intelligence sector long after becoming well established in other areas of the state. In many established democracies, the germination of intelligence oversight systems has followed a common trajectory: certain activities of intelligence services have generated concerns about encroachment on legitimate democratic processes and the exercise of human rights and fundamental freedoms, this has provoked a season of inquiry and soul-searching, and new oversight mechanisms have been created as a result.

Emerging democracies need not take this reactive approach. "Transition" presents them with a gilt-edged opportunity to lay down robust legal and institutional foundations for the oversight of intelligence services. However, we must remain mindful that the establishment of these foundations is but one small step in the interminable and challenging process of ensuring that services are not only effective in protecting national security, public safety and human rights, but also respectful of the rule of law and democratic praxis. Accomplishing these aims on a long-term basis requires ongoing interest, vigilance and dedication on the part of the stakeholders involved in oversight, as well as assiduous efforts to evaluate and improve systems of oversight. I am confident that this toolkit can serve as an important resource in support of this work.

Parliamentarians shoulder great responsibility for both developing the legal and institutional framework for oversight and, as the principal external overseers, for ensuring that oversight accomplishes the aforementioned aims. In this field, more than any other, parliamentarians must strive to subordinate their party political interests to the greater aim of protecting their democratic and constitutional order. Nevertheless, parliamentarians alone should not be saddled with all external oversight responsibilities – they often lack the time, expertise and requisite independence. In view of this, they must call upon independent statutory oversight bodies, such as supreme audit institutions, ombuds institutions and expert oversight bodies, to play a pivotal role in their respective areas of competence.

While there have been many publications focussing on intelligence oversight, the majority of these focus on legal and institutional frameworks for oversight bodies. This toolkit

builds upon this approach by taking decision makers through many of the challenges and conundrums that arise in designing, amending and consolidating a system of oversight. Yet, contributing authors venture beyond questions of design by offering clear practical guidance on how external overseers can tackle the challenges of scrutinising specific areas of intelligence services' work. I hope that this toolkit can also serve to raise awareness amongst civil society and media about the importance of these various aspects of intelligence oversight, and that these groups can use these insights to hold parliamentarians and other independent overseers to account for their scrutiny (or lack thereof) of intelligence services.

This toolkit is likely to be of most interest for decision makers involved in developing intelligence oversight systems, members and staffers of recently-established oversight bodies, as well as civil society organisations. While the majority of such persons may be in transition states, one should not discount the value of the authors' insights to those involved – either directly or indirectly – in intelligence oversight in established democracies. Indeed, I firmly believe that this toolkit provides examples and arguments that will provoke discussions on possible extensions or enhancement of oversight in these polities.

For more than ten years, DCAF has been supporting efforts to strengthen intelligence oversight capacities, not only in emerging democracies but also in more established democratic systems. DCAF views the reform of intelligence oversight systems as an integral part of security sector reform processes in transition settings. While some donors dedicate a substantial share of resources to enhancing the operational capacity of transition states' intelligence services (in order to create effective operational partners), it is of paramount importance that both donor and recipient states invest in developing and maintaining durable and effective systems of oversight. It is my hope that this toolkit can contribute to redressing this balance between operational effectiveness and governance by raising awareness of the indispensability of intelligence oversight amongst the security sector reform community.

Ambassador Theodor H. Winkler
Director, DCAF

Foreword

As a child I was fascinated by kaleidoscopes, and as an adult I still am. All that you hold in your hands is a small tube with at one end a frosted glass sealer and at the other a small round hole. If you carefully shake the tube you usually hear a soft tinkling sound. But you have no idea what is inside it.

When you look through the small hole you see nothing, unless you hold the tube in such a way that the light falls on the frosted glass. It is then that you suddenly see a complex mosaic. And when you turn the tube round you see the pattern of that mosaic changing – fascinating.

In a way, this book looks a little like a kaleidoscope. After all, the intelligence world is a black box that must be dealt with in a certain manner in order to gain insight into it. Moreover, the perspective seems to shift continuously.

What the more observant viewer sees is nevertheless always worthwhile, and also interesting to the extent that the viewer will want to share the insight she/he gains with others. This is, for that matter, not as simple as it seems because the secrets of the tube in which the intelligence world is contained simply may not be revealed just like that.

This book intends to provide a structure to supply tools enabling oversight bodies to hold the tube against the light in the correct way and to subsequently report on what they observed in a well-founded manner.

When describing these tools, the authors shed light on various aspects of oversight, placing the different oversight systems next to one another, thus creating a kaleidoscopic image which does justice to the fact that more than one type of oversight exists, and which invites one to continuously look at the wonderful world of intelligence work with a fresh and critical point of view.

Not only interested outsiders, but certainly also insiders – oversight bodies and those subject to oversight – shall therefore profit from studying this book.

Bert van Delden
Chair, Dutch Review Committee on the Intelligence and Security Services

Acknowledgements

The editors would like to express their gratitude to the Ministry of Foreign Affairs of the Netherlands, whose generous financial support has made this toolkit possible. In particular, we would like to thank the following members of the Security and Defence Policy Department for their invaluable support and cooperation throughout the development of this toolkit: Jacco Bos, Hein Knegt, Michael Stibbe, Frank van Beuningen and Joep Wijnands.

We would also like to acknowledge the contribution of the Dutch Review Committee on the Intelligence and Security Services (CTIVD) and particularly its chair, Bert van Delden; former secretary, Nick Verhoeven; and the Committee's current secretary, Hilde Bos-Ollerman. The CTIVD provided essential support for the initiation of this project and the Committee has generously provided its expertise throughout the development of the toolkit. The editors would also like to record their thanks to former Dutch minister of defence and senator, Wim van Eekelen, whose support for DCAF has been indispensable to the success of this project.

Furthermore, the editors are indebted to Agincourt Press whose staff was responsible for the line editing and copyediting of most of the toolkit. Agincourt Press' staff worked tirelessly to ensure consistency of language and style, as well as to ensure that, are far as possible, the toolkit is accessible to a non-expert audience. We would also like to thank Alice Lake-Hammond for her excellent design work and for her highly professional approach to layouting and typesetting the toolkit.

Finally, we would like to thank our former colleague, Gabriel Geisler Mesevage, who not only co-authored the introductory tool but also made a significant contribution to the conceptualisation and development of the toolkit.

Hans Born and Aidan Wills
Geneva, July 2012

TOOL 1

Introducing Intelligence Oversight

Hans Born and Gabriel Geisler Mesevage

1

Introducing Intelligence Oversight

Hans Born and Gabriel Geisler Mesevage

1. INTRODUCTION

This tool introduces the reader to the subject of intelligence oversight, providing concise answers to the basic questions of who, what, when, how, and why. It also introduces readers to the other tools in this toolkit on intelligence oversight, which collectively provide more elaborate answers to these and other questions.

The goal of this project is to bring together some of the world's foremost experts in the field of intelligence oversight and have them present their expertise in a manner comprehensible to non-experts. This toolkit is specifically intended to help readers strengthen their understanding of relevant issues and expose those with oversight-related responsibilities to a variety of comparative perspectives.

This introductory tool begins with an overview of the intelligence oversight process, including descriptions of the institutions involved and of the "intelligence oversight cycle." Next, it explains why intelligence oversight is important for protecting individuals' human rights and fundamental freedoms, as well as for increasing their security. The tool then surveys current standards and practices in intelligence oversight, focusing on what most experts consider to be good practices. The tool concludes with recommendations for the strengthening of intelligence oversight.

1.1 WHY AN INTELLIGENCE OVERSIGHT TOOLKIT?

This toolkit was created to help emerging democracies establish—and established democracies improve—civilian oversight of intelligence services. It has four principal aims:

1. to provide policy-relevant guidance on the creation and consolidation of new oversight systems as well as the review and improvement of existing systems.
2. to provide guidance on the oversight of particular areas of intelligence services' activities including information collection, use of personal data, and information sharing.
3. to generate awareness of the importance of intelligence oversight among members of civil society and the media.
4. to promote cross-national learning and norms transfer through the identification and analysis of different approaches, standards, and practices of intelligence oversight.

Thus, the emphasis in this toolkit is placed not on abstract academic analysis but on the presentation of practical guidance to those who oversee and/or interact regularly with intelligence oversight systems. It is for this reason that we have chosen to use the toolkit format, with its focus on practical examples and specific recommendations reflecting practices the world over.

1.2 ISSUES ADDRESSED IN THE TOOLKIT

The nine tools in this toolkit are self-contained introductions to important issues in intelligence oversight (see Table 1). Each has been written so that it can be read on its own.

1.3 THE INTENDED AUDIENCE

This toolkit is intended primarily for those who are directly or indirectly involved in intelligence oversight. Such an audience includes members of the executive, legislative, and judicial branches of government and their staffs; intelligence officials; members of civil society; and members of the media.

We are confident that this toolkit's contents are of broad public interest. Yet there are particular constituencies that will find the tools especially useful. For instance, because the tools examine closely the roles played by parliamentary and expert oversight bodies, members and employees of these institutions will find the information in the toolkit particularly relevant. Similarly, journalists and members of civil society whose work encompasses the analysis of intelligence services will find much that is helpful in the tools, as will government officials currently engaged in creating or reforming intelligence oversight systems.

TABLE 1: OVERVIEW OF THE TOOLS

Tool	Title	Main questions addressed
1	Introducing Intelligence Oversight	▪ What is intelligence oversight? ▪ Why is intelligence oversight important? ▪ What are responsibilities of the various institutions involved in intelligence oversight?
2	Establishing Effective Intelligence Oversight Systems	▪ What are the advantages and disadvantages of various institutional approaches to intelligence oversight? ▪ What are the impediments to effective oversight, and how can they be addressed? ▪ What are the principal considerations when designing legal and institutional frameworks for intelligence oversight?
3	Intelligence Transparency, Secrecy, and Oversight in a Democracy	▪ What is a proper balance between secrecy and transparency for intelligence services in a democracy? ▪ What is good practice regarding legislation on the protection of and access to information? ▪ What are the intelligence information needs of parliament, specialized oversight bodies and the public?
4	Conducting Oversight	▪ What approaches and methods are used by oversight bodies to hold intelligence services accountable? ▪ How can oversight bodies conduct effective investigations into the practices of intelligence services? ▪ How can oversight bodies report on their investigations?
5	Overseeing Information Collection	▪ Why is oversight of the information collection process important? ▪ How can oversight bodies monitor the information collection process effectively? ▪ What are the impediments to effective oversight of the information collection process, and how can they be addressed?
6	Overseeing the Use of Personal Data	▪ Why is oversight of the use of personal data important? ▪ How can oversight bodies ensure that intelligence services use personal data only in ways that comply with the law? ▪ What are the impediments to effective oversight of the use of personal data, and how can they be addressed?
7	Overseeing Information Sharing	▪ Why is oversight of information sharing important? ▪ What role should oversight bodies play with regard to information sharing? ▪ What are the impediments to effective oversight of domestic and international information sharing, and how can they be addressed?
8	Financial Oversight of Intelligence Services	▪ Why is oversight of the finances of intelligence services important? ▪ What is required for intelligence services to be financially accountable? ▪ What are the roles and responsibilities of various institutions involved in the financial oversight of intelligence services?
9	Handling Complaints about Intelligence Services	▪ Why are complaint-handling mechanisms important? ▪ What types of complaint-handling systems exist? ▪ How can complaint-handling systems be improved?

2. WHAT IS INTELLIGENCE OVERSIGHT?

This section outlines the scope and context of intelligence oversight and discusses the institutions involved. For reasons of conciseness and clarity, this toolkit uses the generic term intelligence service to refer to entities that are variously called "security services," "security intelligence services/organizations," and "intelligence agencies."[1] Because different jurisdictions structure intelligence work in different ways, this toolkit takes a functional approach to the definition of *intelligence service*. Specifically, it defines an intelligence service as a state organization that collects, analyzes, and disseminates information related to threats to national security.

Such a definition covers a wide variety of organizations—including military intelligence, police intelligence, and civilian intelligence services, both domestic and foreign. It also includes often-overlooked organizations frequently housed in finance ministries and treasury departments, such as agencies tasked with the investigation of terrorist financing or the prevention of money laundering. As *The OECD DAC Handbook on Security Sector Reform* relates,"Most countries have a multitude of intelligence organisations that have specific, sometimes overlapping responsibilities. These include internal and external intelligence, tactical and strategic intelligence, criminal intelligence, collection agencies (for example, communications, human intelligence and imagery), civilian and military intelligence, and strategic assessment bodies."[2] Taken together, these agencies comprise the "intelligence community."

Intelligence services can also be distinguished from other government agencies by the special powers they possess to collect information—such as the power to intercept communications, the power to conduct covert surveillance, the power to make use of secret informants, and the power to enter dwellings surreptitiously. In some states (such as Denmark, Malaysia, Russia, and Sweden), intelligence services possess police powers as well and are therefore sometimes called "police security services" or "special branches." In other states, the work of police services is completely separated from the work of intelligence services: the latter do not have any police powers (e.g. to arrest, detain, and interrogate suspects).

Although the definition we have used restricts intelligence services to organizations of the state, there are some countries in which the government employs private contractors to carry out intelligence work.[3] Because the oversight of private contractors differs substantially from that of public services, it is not discussed in this toolkit.

2.1 THE SCOPE OF INTELLIGENCE OVERSIGHT

Oversight is a catchall term that encompasses *ex ante* scrutiny, ongoing monitoring, and *ex post* review, as well as evaluation and investigation. It is performed by managers within the intelligence services, by executive officials, by members of the judiciary and members of parliament, by independent ombuds institutions, by audit institutions, by specialized oversight bodies, by journalists, and by members of civil society.

Oversight should be distinguished from *control* because the latter term (like management) implies the power to direct an organization's policies and activities. Thus, *control* is typically associated with the executive branch of government and specifically with the senior management of intelligence services. An example of control, as opposed to

oversight, would be the issuance of an executive order requiring an intelligence service to adopt a new priority, such as counterterrorism. Readers should be aware, however, that not every government makes a clear distinction between oversight and control. For this reason, some institutions described in this toolkit as oversight bodies may also possess a number of control responsibilities.

The main purpose of oversight is to hold intelligence services to account for their policies and actions in terms of legality, propriety, effectiveness, and efficiency.[4] The process by which an oversight body holds an intelligence service accountable has usually three distinct phases:

1. The oversight body collects information about the intelligence service.
2. Based on this initial information, the oversight body engages in a dialogue with the intelligence service.
3. The oversight body issues findings and recommendations.

Thus, in order to function effectively, an oversight body must posses the ability to access relevant information, to question intelligence officials, and to issues findings and recommendations on the basis of what it learns. Without these three powers, there can be no real accountability, and intelligence oversight is likely to fail.

Oversight can encompass not only the propriety and legality of a service's activities but also the service's effectiveness and efficiency. In this context, *propriety* refers to whether an intelligence service's actions are morally justified, while *legality* refers to whether those actions comply with governing law. *Effectiveness* measures the extent to which a service realizes its goals, while *efficiency* measures how economically a service pursues those goals. In some states, intelligence oversight bodies concern themselves exclusively with legality (for example the Dutch Review Committee on the Intelligence and Security Services); in other states, the law mandates oversight bodies to focus exclusively on effectiveness and efficiency (for example the Intelligence Security Committee in the United Kingdom).

2.2 INSTITUTIONAL RESPONSIBILITIES

Effective intelligence oversight requires not only the coordinated activity of several state bodies but also the active review of governmental conduct by members of civil society and the media. Although all of these bodies play important roles, this toolkit focuses primarily on parliamentary and expert oversight bodies because these bodies answer neither to the intelligence services nor to the executive, which means that they are better placed to independently safeguard democratic accountability and respect for the rule of law and for human rights.

Table 2 offers an overview of the responsibilities generally assumed by public and private bodies in the oversight process. Readers should note, however, that these responsibilities are managed differently in different countries and that the oversight system of a particular state may not address all of the responsibilities identified in the table.

TABLE 2: OVERSIGHT BODIES AND THEIR KEY RESPONSIBILITIES

Oversight bodies	Key responsibilities
Senior management of the intelligence services	▪ Implementing and monitoring adherence to internal controls ▪ Fostering an institutional culture that promotes respect for the rule of law and for human rights ▪ Reviewing requests for the use of special powers and applying to external bodies for the necessary permission ▪ Ensuring cooperation with internal and external oversight bodies ▪ Enforcing rules that prohibit illegal orders and supporting officers who refuse to obey those orders ▪ Implementing and monitoring procedures to protect whistleblowers
Executive	▪ Appointing senior intelligence service management ▪ Establishing intelligence service policies and priorities and issuing guidelines ▪ Reporting to the parliament on the activities of the intelligence services ▪ Ensuring that the intelligence services cooperate with other intelligence oversight bodies ▪ Formulating intelligence service budgets and examining service expenditures ▪ Approving intelligence service cooperation with other services and agencies, both domestic and foreign ▪ Authorizing requests for the use of special powers ▪ Approving sensitive intelligence operations
Parliamentary and expert oversight bodies	▪ Adopting and amending a comprehensive legal framework for the intelligence services and its oversight ▪ Evaluating the propriety, legality, effectiveness, and efficiency of intelligence service activities ▪ Approving and reviewing intelligence service budgets
Judiciary	▪ Authorizing *ex ante* and/or reviewing *ex post* the use of special powers by the intelligence services ▪ Adjudicating criminal, civil, constitutional, and administrative law cases that concern the activities of the intelligence services ▪ Serving as members of expert oversight bodies and independent, ad hoc inquiries (in a personal capacity)
Ombuds institutions	▪ Hearing complaints against intelligence services ▪ Initiating thematic investigations of intelligence service activity
Supreme audit institutions	▪ Revealing problems with legality, efficiency, and effectiveness in financial management as well as making recommendations for the improvement of financial management ▪ Assuring the parliament of the accuracy and regularity of government accounts, thereby helping to ensure that the executive complies with the will of the parliament ▪ Assuring the public that its money is being spent lawfully, appropriately, efficiently, and effectively
Civil society and the media	▪ Investigating the policies and activities of the intelligence services and the intelligence oversight bodies ▪ Exposing improper, illegal, ineffective, or inefficient conduct on the part of the intelligence services ▪ Keeping the public informed regarding intelligence service policies, activities, and its oversight ▪ Encouraging public debate about the policies and activities of intelligence services and about the work of intelligence oversight bodies

2.2.1 Senior management of the intelligence services

Effective intelligence oversight begins with effective internal controls. Executive branch officials, parliamentary committees, and expert bodies will all have difficulty fulfilling their oversight responsibilities if the senior management of an intelligence service is lax and/or uncooperative. On the other hand, if senior management is engaged and supportive, internal service controls and management systems can provide important safeguards against the abuse of power and the violation of human rights.

Implementing and monitoring adherence to internal controls

Senior management has the direct responsibility for developing and maintaining adherence to internal controls—which the Venice Commission has defined as "decision-making structures designed to make sure that measures and policies are properly authorized."[5] Put another way, internal controls hold intelligence officers accountable for their conduct within their service's legal mandate, the priorities set for the service by the executive, and the policies and regulations established by senior service management. Internal controls also include procedures for proper budgeting and record keeping.

Fostering an institutional culture that promotes respect for the rule of law and for human rights

The need for intelligence services to foster and maintain institutional cultures that respect the rule of law and human rights is widely acknowledged.[6] Laws and regulations promoting such cultures are therefore important, but they are not sufficient. Senior service management must also develop and conduct programmes designed to instill in their employees an understanding of constitutionality, legality, accountability, and integrity.

Reviewing requests for the use of special powers and applying to external bodies for the necessary permission

In most states, the use of special powers by an intelligence service is ultimately subject to ministerial and/or judicial approval because of the impact such powers can have on human rights. The service's senior management, however, plays a critical role in deciding which requests merit being passed along to these external bodies. Management should make such decisions balancing the intrusiveness of the operation against the nature of the threat. Greater risks to human rights should require higher levels of internal authorization.

Ensuring cooperation with internal and external oversight bodies

Senior service management is responsible for the effective functioning of all internal oversight bodies. This responsibility includes ensuring that service employees cooperate fully with internal oversight bodies as well as with external oversight bodies. Furthermore, senior management should insulate (in particular internal) oversight bodies from administrative pressures so that they can function effectively as complaint-handling mechanisms.

Enforcing rules that prohibit illegal orders and supporting officers who refuse to obey those orders

Senior management must take all necessary actions to ensure that illegal orders are not given; and that if they are given, that they are not obeyed. This can be bolstered by whistleblower protection laws that allow intelligence service personnel to reveal

information showing wrongdoing to designated internal or external bodies. In some states, legal procedures have been created for the reporting of questionable intelligence activity to the director of the intelligence service or another relevant official. In Bosnia and Herzegovina, questionable activity is reported to the service's inspector general (see Box 1). In other countries, it is reported to the responsible minister.[7] In addition, the national laws of some state (such as Bulgaria[8]) hold intelligence service employees individually accountable for illegal actions and/or for violations of their official duties.

Box 1: The duty of intelligence officers to report illegal activity in Bosnia and Herzegovina

"Should an employee believe that s/he has received an illegal order, s/he shall draw the attention of the issuer of the order to his/her concerns with respect to its illegality. In cases where the issuer of the order repeats the order, the employee shall request a written confirmation of such order. If the employee continues to have reservations, s/he shall forward the order to the immediate superior of the issuer of the order and report the matter to the Inspector General. The employee may refuse to carry it out."[9]

2.2.2 Executive

The doctrine of ministerial accountability[10] prescribes that each minister is accountable to the head of state, the cabinet, and the parliament for the exercise of his or her powers and functions.[11] Under this doctrine, the executive, which sets policy for the intelligence services, is politically responsible for their conduct.

Typically, intelligence services report to a government minister who is responsible for ensuring that the service functions in a proper, legal, effective, and efficient manner. In Germany, for example, the foreign, domestic, and military intelligence services report respectively to the head of the Federal Chancellery, the minister of the interior, and the minister of defence.[12]

The degree of control exercised by the executive varies from state to state. The complexity of intelligence work can make it difficult for the executive to monitor and control service behavior. Indeed, "the monopoly of specialist knowledge possessed by the agency," the Venice Commission has observed, "will itself grant the agency a considerable degree of autonomy in practice from governmental control."[13]

Although executive officials have a strong interest in avoiding intelligence failures, they do not have an equally strong interest in revealing failures when they occur. Public disclosure of service mishaps or wrongdoing can cause political embarrassment and negatively affect the careers of the ministers involved. For this reason, some experts mistrust the ability of the executive to perform proper oversight of the intelligence services and rely instead on the review and critique of executive decision making by the parliament, the judiciary, and civil society.

Despite this concern, the executive nevertheless embodies an important link in the chain of accountability. The responsibilities listed in Table 2 make clear that, in addition to political responsibilities, the executive also has operational responsibilities with regard to the intelligence services, especially concerning the implementation of policy. For this reason, it is important that information concerning difficult or sensitive operational

decisions not be withheld from members of the executive. To the contrary, the executive should always be informed.

2.2.3 Parliamentary and expert oversight bodies

Just as it is crucial to establish and maintain effective oversight of security intelligence activities on the executive side of government, it is also essential to have independent oversight, both parliamentary and non-parliamentary. The secrecy of intelligence work, its lack of exposure to judicial examination and comment, the threat to human rights posed by excessive surveillance, and the record of past wrong-doings all point to the need for effective oversight of intelligence services by bodies independent of the government of the day.[14]

In general, parliamentary oversight committees and expert bodies provide the most effective external oversight. The former can be helpfully divided into two categories: general committees with broad mandates (such as defence and foreign affairs committees) and specialized committees whose sole focus is the intelligence community. Although general committees (especially in the areas of budget and finance) may have particular oversight responsibilities with regard to the intelligence services, the bulk of intelligence oversight is typically conducted by specialized committees because of the greater experience and expertise of their members and because this approach limits the circle of knowledge and information to committee members rather than all members of parliament.

Expert intelligence oversight bodies (sometimes called "specialized oversight institutions" or "specialized non-parliamentary oversight bodies") are set up and function independently from the executive, parliament and the intelligence services they are mandated to oversee. Expert oversight bodies similarly benefit from the expertise of their members and the precision of their focus. In most states, such bodies are populated with intelligence experts who may include former or current judges, prosecutors, and heads of police services.[15] Indeed, the members of expert oversight bodies often have greater experience and expertise than the members of specialized parliamentary committees. Furthermore, members of expert bodies usually have the freedom to devote themselves entirely to intelligence oversight, whereas parliamentarians sit on several committees and must therefore manage multiple responsibilities. Another advantage of expert oversight bodies is that their members are neither professional politicians nor directly involved in day-to-day political activity, thus their conduct tends to be much less politicized than that of parliamentarians. Nevertheless, expert oversight should always be viewed as a complement to, not a substitute for, parliamentary oversight, because the principles of democratic governance require direct scrutiny by the parliament of all government operations.

Some states (such as Australia, see Box 2) have strengthened intelligence oversight by establishing an independent inspector general. The name, mandate, powers, and functions of this office vary considerably from state to state (see Farson—Tool 2), but its core missions typically include ensuring that intelligence services comply with the constitution, statutory law, and operational policies set by the executive. Other common functions include:

- educating intelligence service personnel about their rights and responsibilities
- carrying out internal audits and inspections—especially for the purpose of detecting and preventing waste, fraud, and abuse

- ensuring the maintenance of effective security policies and procedures
- receiving and investigating complaints made by service personnel
- ensuring the release of information to which members of the public are entitled by freedom of information legislation
- ensuring that service record keeping complies with relevant legislation and policies[16]

Box 2: The Australian Inspector General of Intelligence and Security

The Australian Inspector General (IG) of Intelligence and Security provides independent assurance to the prime minister, senior ministers, and the parliament that the country's intelligence services and other security agencies are acting legally and with propriety. The IG provides such assurance by investigating the intelligence services and security agencies and reporting on their activities. The IG's mandate further includes the responsibility to monitor whether the intelligence services and security agencies are operating effectively and whether they are showing respect for human rights.

To fulfill this mandate, the IG is empowered by Australian law to conduct inquiries at the request of the responsible minister or on the IG's own initiative. In addition, the IG is empowered to receive and investigate complaints made by people affected by intelligence service activity. Such investigations may include the inspection of intelligence service premises (such as places of detention); the taking of testimony under oath; and access to documents. At the conclusion of each inquiry, the IG provides a report to the responsible minister, a summary of which is usually included in the IG's annual report to the Australian parliament. The director of the service concerned and the responsible minister are legally bound to report to the IG on the implementation of any recommendations contained in the IG's report.[17]

The mandates of parliamentary oversight committees and expert oversight bodies vary from state to state. Some countries (such as the United States with its congressional intelligence oversight committees) have enacted mandates that cover the full spectrum of propriety, legality, effectiveness, and efficiency; other countries (such as the Netherlands and Sweden) limit the mandates of such bodies to legality only.

So that parliamentary oversight committees and expert oversight bodies can fulfill these mandates, they are often granted far-reaching powers, which may include any or all of the following (non-exhaustive) list:

- the power to access classified information
- the power to receive and review annual and other reports produced by the intelligence services
- the power to subpoena executive and intelligence officials to testify under oath
- the power to invite external experts and other members of the public to testify under oath
- the power to meet periodically with the responsible ministers and/or the directors of the services
- the power to conduct both regular and ad hoc inspections and to visit the premises of the intelligence services

2.2.4 Judiciary

Because intelligence services are not above the law, they fall within the jurisdiction of the courts. Although the role of the courts with regard to intelligence work deserves more detailed attention than can be provided here, the following brief comments may be helpful.

Although the judiciary has a responsibility to uphold the rule of law and ensure respect for human rights, judges have traditionally deferred to the executive on matters of national security for two reasons. First, constitutions and governing law often place matters of national security within the exclusive purview of the executive. Second, many judges perceive the courts as ill-suited venues for the disclosure of confidential information.[18] Even so, some court systems do play active roles in intelligence oversight. In the United States, for instance, the expansion of criminal defendants' due-process rights has led judges to examine governmental behavior in ever-greater detail, and the Congress increasingly passed intelligence-related legislation that has also contributed to increased judicial review.[19] In other countries, especially where the executive has been making excessive and overbearing claims in the name of national security, judges have become more active in upholding the constitutional and human rights.[20]

Judicial oversight of intelligence services takes place in four primary ways, three of which extend beyond oversight into the realm of control. First, governing law often requires intelligence services wishing to use special investigative measures (such as the interception of communications) to seek *ex ante* authorization from a judge or to submit to *ex post* judicial review. Such requirements are important because they place an independent check on the legality of intrusive service activities. Second, judges can be called on to preside over criminal trials involving intelligence work–related offences and to adjudicate claims—constitutional, civil, or administrative—involving intelligence-related matters. Third, in some states (such as France), investigating magistrates who specialize in security issues can be given supervisory control over intelligence service investigations. Fourth, judges may occasionally become members of oversight bodies or be asked to chair ad hoc commissions of inquiry.

The first three of these roles qualify as means of control because they give judges the power to direct the activities of the intelligence service involved. The fourth role, in comparison, is more limited, usually lacking the power to issue binding recommendations.

2.2.5 Ombuds institutions

The most common interaction between ombuds institutions and the intelligence community is the handling of complaints made against intelligence services by members of the public. In the Netherlands, for instance, anyone can file a complaint with the national ombudsman on matters relating to "the actions or the alleged actions of the relevant Ministers, the heads of the [intelligence] services, the coordinator and the persons working for the services and for the coordinator."[21] Initially, the complainant must inform the responsible minister, who then seeks the advice of the Review Committee on the Intelligence and Security Services (CTIVD). Next, the Dutch national ombudsman investigates the complaint and renders "his decision on the complaint in writing to the person filing the complaint and, insofar as the security or other vital interests of the state do not dictate otherwise, stating his reasons."[22]

Ombuds institutions tend to have both the virtue of independence and the legal powers necessary to access information pertinent to their investigations. Unfortunately, they also tend to have staffs that are too small to cover effectively their broad areas of jurisdiction, which frequently encompass not merely the intelligence community but also the armed forces and sometimes the entire government. Consequently, ombuds institutions often suffer from an inability to devote sufficient expertise and resources to intelligence oversight.

2.2.6 Supreme audit institutions

Like ombuds institutions, supreme audit institutions (SAIs) provide independent, external checks on the conduct of intelligence services. Specifically, they monitor the financial aspects of intelligence work, assessing whether service record keeping is fair and accurate, whether internal controls on expenditures are functioning properly, and whether service expenditures comply with prevailing regulations (see Wills—Tool 8). Beyond these responsibilities, SAIs sometimes make value-for-money assessments so that legislators and members of the executive can make informed decisions about how best to structure intelligence service budgets and priorities.

2.2.7 Civil society and the media

Although admittedly an amorphous concept, *civil society* is generally understood to encompass autonomous organizations that exist in the public space between the institutions of state and the private lives of individuals and communities. Such a definition includes, for example, academia, non-governmental organizations (NGOs), advocacy groups, and religious orders. A great advantage of civil society organizations in conducting intelligence oversight is that their ability to analyze and critique government policies is unrestricted.

Like civil society organizations, media entities make use of independent (that is, non-governmental) expertise to provide constant feedback on the actions of intelligence services. Investigative journalists, in particular, play a crucial role in revealing improper, illegal, ineffective, and/or inefficient intelligence service conduct. Once revealed, these instances of failure or wrongdoing often become the subject of formal inquiries led by parliamentary committees or other independent oversight bodies, such as expert oversight bodies, ombuds institutions or supreme audit institutions (SAIs). Without media reports calling attention to these matters, they might never be investigated.

Whether revelations of malfeasance or simply accounts of executive policy, media reports also tend to place particular issues on the agenda of the government by making them topics of public debate. For instance, the *Washington Post's Top Secret America* series publicized the startling growth of the US intelligence community in the decade following the September 11, 2001, attacks, igniting a vigorous public debate on the cost-effectiveness of such an investment.[23] However, it must be acknowledged that highly politicized or biased journalism can be deleterious to intelligence oversight.

2.3 THE INTELLIGENCE OVERSIGHT CYCLE

Oversight can occur at several different points in time. It can occur at the outset of an operation that has been proposed but not yet undertaken (*ex ante* oversight), it can occur

while the operation is under way (ongoing oversight), or it can occur after the operation has concluded (*ex post* oversight).

2.3.1 *Ex ante* oversight

The most common *ex ante* oversight activities include: the creation of comprehensive legal frameworks for the intelligence services and the bodies that oversee them; the creation and approval of budgets for the intelligence services; and the authorization of intelligence operations that exceed a certain threshold of sensitivity.

For legal frameworks to be effective, they must state clearly the mandate of the service or oversight body and the powers to which the service or body is entitled. Although perhaps not oversight in the conventional sense, this legislative activity is a starting point (and a sine qua non) for any useful oversight system. Without clearly defined mandates and powers, intelligence services and oversight bodies cannot function properly. (The creation of legal frameworks is discussed extensively in Farson—Tool 2).

Government agencies cannot operate without funds. Thus, the parliament, which in a democracy controls the use of public funds, must enact annual budgets for all government agencies, including the intelligence services. Proposed budgets are typically submitted to the relevant parliamentary committee by the responsible minister acting in consultation with the senior management of the services; the treasury; and, in some cases, the supreme audit institution. (The budgetary process is discussed in greater detail in Wills—Tool 8.) The members of the parliamentary committee then assess the proposed budget in terms of current executive intelligence policy. Not surprisingly, parliamentarians frequently use the budgetary process as an opportunity to critique executive policy and the priorities the executive has set for the intelligence services.

Intelligence activities that require prior authorization usually involve the use of special powers that infringe on individual rights, such as the electronic surveillance of personal communications. Most often, this form of *ex ante* oversight is performed by a judge, but in certain situations it may be performed by a non-judicial or quasi-judicial oversight body such as the G10 Commission of the German *Bundestag* (named after Article 10 of the German Basic Law, which concerns postal and telecommunications privacy). (See Hutton—Tool 5).

2.3.2 Ongoing oversight

Ongoing oversight can include investigations, on-site inspections, periodic hearings, and regular reporting on the activities of the intelligence services and of the oversight bodies themselves. In addition, in some states, judges periodically review ongoing information-collection operations, such as wiretaps, to determine whether continuation of the operation is justified.

In 2011, the Dutch Review Committee on the Intelligence and Security Services (CTIVD) reported that its ongoing oversight activities included regular reviews of service wiretaps, service security screenings, and the processing of applications requesting access to service files. In addition, the Review Committee investigated whether the services had fulfilled their legal obligation to notify individuals who had been subjected to the use of special investigatory measures.[24] Another intelligence oversight body with a specific mandate

to conduct ongoing oversight is the Norwegian Parliamentary Intelligence Oversight Committee (see Box 3).

Box 3: The Norwegian Parliamentary Intelligence Oversight Committee

The activities of the Norwegian Parliamentary Intelligence Oversight Committee (EOS Committee) are stipulated in the Act Relating to the Monitoring of Intelligence, Surveillance, and Security Services of 3 February 1995. This legislation establishes the EOS Committee as "purely monitory."[25] Accordingly, "The Committee may not instruct the monitored bodies or be used by these for consultations."[26]

Section 3 of the law states that the EOS Committee "shall regularly monitor the practice of intelligence, surveillance and security services in public and military administration." Section 4 permits the committee, in fulfillment of this mandate, to enter premises, and Section 5 allows the committee to compel witnesses to appear before it at hearings.

Furthermore, Section 8 obligates the committee to issue an unclassified report in response to any complaint it receives and to issue annual reports to the Storting (the Norwegian parliament) describing its activities. In addition, the committee may issue periodic reports on particular topics if "factors are revealed that should be made known to the Storting immediately."[27] This latter power allows the EOS Committee to conduct important ongoing oversight of the activities of the Norwegian intelligence services.

2.3.3 *Ex post* oversight

The most common forms of *ex post* oversight are thematic reviews, case reviews, expenditure reviews (see Wills—Tool 8), and annual reviews. In certain situations, however, such as when alleged wrongdoing is revealed, *ex post* oversight can take the form of an ad hoc inquiry. Such inquiries are normally established to investigate and make recommendations concerning specific events.

In 2004, for instance, the Canadian government launched a special inquiry into the role played by the Royal Canadian Mounted Police (RCMP) in the case of Maher Arar, a Canadian citizen whose rendition by the United States to Syria resulted in his torture (see Roach—Tool 7). The inquiry had two aspects: a factual review and a policy review. The goal of the factual review was to "investigate and report on the actions of Canadian officials in relation to what happened to Maher Arar."[28] The goal of the policy review was to "make recommendations for an independent, arm's-length review mechanism with respect to the RCMP's national security activities."[29] Structuring *ex post* investigations in this two-part manner is useful, because it both establishes the truth of what has transpired and provides an opportunity for the formulation of appropriate policy responses.

Another important area of *ex post* oversight is the handling of complaints (see Forcese—Tool 9),[30] which can be managed in a variety of institutional formats. Often, complaints are handled by the judiciary, but they can also be handled non-judicially, such as by ombuds institutions (e.g. in Serbia), parliamentary committees (as in Hungary), or by expert oversight bodies (as in Norway).

2.4 ASSESSING INTELLIGENCE OVERSIGHT

Intelligence oversight bodies assess the performance of the intelligence services, but who assesses the performance of the oversight systems, and how is that performance assessed? Intelligence overseers and academics have only recently begun to take up these questions, because, among other factors, in many states intelligence oversight systems were not established until the 1990s.

A few countries have subjected their intelligence oversight systems to external evaluation. In Canada, a special committee of the House of Commons did so as part of a five-year review of the Canadian Security Intelligence Service Act;[31] while in the Netherlands, at the request of the CTIVD, an independent expert conducted a similar review of the Intelligence and Security Services Act.[32] In addition, some countries have evaluated their oversight systems as part of parliamentary or independent inquiries into alleged intelligence service failures or wrongdoing. Examples of these include the 9/11 Commission in the United States and the Arar inquiry in Canada.

The following principles may guide future research into this important topic, whose full complexity is beyond the scope of this toolkit:

- Governing law should mandate periodic reviews of the intelligence oversight system to determine whether it is still fit for its purpose.
- These periodic reviews should encompass the entire oversight system—including senior intelligence service management, the executive, the parliament, the judiciary, independent oversight bodies, civil society, and the media.
- Such reviews should determine whether the mandates of the intelligence oversight bodies, when assessed collectively, cover the most important aspects of intelligence service activity. In particular, they should determine whether the mandates cover both the legality and the effectiveness of service conduct.
- Evaluations of specific oversight bodies should focus on the oversight body's ability to hold accountable the services it oversees. In other words, are the powers and resources of the oversight body sufficient to execute its mandate? Specifically, is the body sufficiently independent of the executive and the intelligence services, does it have sufficient access to classified information, does it possess the necessary investigative powers, and does it have enough expert staff?

3. WHY IS INTELLIGENCE OVERSIGHT IMPORTANT?

The three main reasons that states create intelligence oversight systems are to enhance democratic governance of the intelligence services (including their accountability to the electorate), to uphold the rule of law, and to ensure the effectiveness and efficiency of service activity.

3.1 DEMOCRATIC GOVERNANCE AND ACCOUNTABILITY

One of the fundamental principles of democratic governance is the accountability of state institutions to the electorate. Furthermore, because intelligence services make use of public funds, the public has a right to know whether those funds are being used in a proper, legal, effective, and efficient manner.

Given the confidential nature of much intelligence work, intelligence services cannot be fully transparent; thus, society must create an alternate mechanism (other than public scrutiny) to monitor the behavior of the intelligence services on behalf of the electorate. The most common mechanisms are parliamentary committees and expert oversight bodies created by the parliament in fulfillment of its obligation to ensure that suitable checks and balances exist to control all government agencies.

Such checks and balances need to ensure, in particular, that intelligence services act in defence of national security and not the security of the incumbent government. Indeed, intelligence services should never act as a tool of a political party but only as a servant of the public.

Democratic governance can also bolster public confidence in the work of intelligence services if the general public knows that the services are properly overseen by its representatives in parliament and by other intelligence oversight bodies.

3.2 UPHOLDING THE RULE OF LAW

Intelligence services, like any other government agency, are obligated to respect and uphold the rule of law. Even the existence of a threat to national security is not sufficient reason for an intelligence service to break the law. Illegal activity on the part of an intelligence service not only violates the rule of law that the service is obligated to protect but also brings the service and the government into disrepute domestically and internationally. In particular, the use of special powers by intelligence services needs to be closely monitored because of the potential that exists for the violation of human rights.

In those countries where intelligence services have been historically associated with law breaking and human rights abuses, close oversight is especially important, not only to discourage the recurrence of wrongdoing but also to build public confidence and trust in the services and the government.

3.3 EFFECTIVENESS AND EFFICIENCY

Because intelligence services play a vital role in protecting national security and because their resources are limited, it is important that those resources be used effectively and efficiently rather than wastefully and without purpose. Thus, a well-designed intelligence oversight system needs to monitor whether the intelligence services are indeed deploying their resources in a manner that achieves the priorities set for them by the executive while obtaining the most value for the taxpayer money spent.

Typically, service efficiency is reviewed both by the parliament during budgetary hearings and by the supreme audit institution during its regular expenditure reviews. The secretive nature of intelligence work makes it easier for intelligence services (as compared to other government agencies) to hide instances of fraud and waste; therefore, oversight bodies must scrutinize the use of public funds especially closely (see Wills—Tool 8).

4. GOOD PRACTICES

Every state needs to ensure that its intelligence services act in a manner consistent with its international legal obligations, including those outlined in the UN Charter and the International Covenant on Civil and Political Rights. Depending on the service's mandate, international agreements regarding the use of police powers may also be applicable.
One way to manage these obligations is to follow good practices. In this toolkit, *good practices* means national and international legal provisions as well as national institutional structures, procedures, and models that promote effective intelligence oversight.

Because there is no one-size-fits-all model for intelligence oversight, it cannot be reasonably claimed that a single standard or practice is unarguably the best. Rather, a diversity of equally good models and approaches can be found in states all over the world. Translating good practices from one state to another can be difficult because of differences in legal, political, and cultural systems; and even when possible, the process usually requires adapting the practices before they can be meaningfully applied. Nevertheless, it is possible to identify common standards and practices that contribute to effective intelligence oversight.

In 2010, DCAF prepared for the UN special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism a catalogue of good practices for intelligence oversight based on a comparative analysis of the constitutions, laws, decrees, parliamentary resolutions, independent inquiries, and court rulings of more than fifty states. (See Box 4).

Box 4: The United Nations compilation of good practices on intelligence oversight

In 2010, based on research by DCAF, the UN special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism presented a compilation of good practices on intelligence services and their oversight.[33] While the compilation includes thirty-five good practices concerning the legal basis, oversight and accountability, respect for human rights, and intelligence functions, the list below only refers to good practices concerning intelligence oversight.

PRACTICE 6. Intelligence services are overseen by a combination of internal, executive, parliamentary, judicial, and specialized oversight institutions whose mandates and powers are based on publicly available law. An effective system of intelligence oversight includes at least one civilian institution that is independent of both the intelligence services and the executive. The combined remit of oversight institutions covers all aspects of the work of intelligence services, including their compliance with the law; the effectiveness and efficiency of their activities; their finances; and their administrative practices.

PRACTICE 7. Oversight institutions have the power, resources, and expertise to initiate and conduct their own investigations, as well as full and unhindered access to the information, officials, and installations necessary to fulfill their mandates. Oversight institutions receive the full cooperation of intelligence services and law enforcement authorities in hearing witnesses, as well as obtaining documentation and other evidence.

PRACTICE 8. Oversight institutions take all necessary measures to protect classified information and personal data to which they have access during the course of their work. Penalties are provided for the breach of these requirements by members of oversight institutions.

5. RECOMMENDATIONS

- Effective oversight systems make use of both internal and external bodies—including senior service management, the executive, the judiciary, parliamentary committees, expert bodies, ombuds institutions, supreme audit institutions, civil society, and the media.
- Taken together, the mandates of the bodies that make up the intelligence oversight system should cover the propriety, legality, effectiveness, and efficiency of the entire intelligence community.
- At least one body in the intelligence oversight system should be civilian, independent, and external to both the intelligence services and the executive.
- Exactly what constitutes an intelligence service should be defined in a functional manner. That is, any state organization whose primary tasks are the collection, analysis, and dissemination of national security information is an intelligence service.
- The monitoring of service activity should cover the full intelligence oversight cycle consisting of *ex ante*, ongoing, and *ex post* oversight.
- The effectiveness of the intelligence oversight system should be assessed regularly by independent bodies.
- Intelligence oversight bodies should communicate regularly with foreign counterparts in order to identify and share good practices.

Endnotes

1. This toolkit uses the term *intelligence service*, rather than *intelligence agency* or *intelligence body*, to emphasize that these organizations perform a public service.
2. Organisation for Economic Co-operation and Development, OECD DAC *Handbook on Security System Reform: Supporting Security and Justice* (Paris: OECD, 2007), p. 140.
3. For information on private contractors, see Tim Shorrock, *Spies for Hire: The Secret World of Intelligence Outsourcing* (New York: Simon & Schuster, 2008).
4. For a fuller discussion of what it means to hold a public agency accountable, see Mark Bovens, "Public Accountability," in *The Oxford Handbook of Public Management*, eds. Ewan Ferlie, Laurence E. Lynne Jr, and Christopher Pollitt (Oxford: Oxford University Press, 2005).
5. Council of Europe, European Commission for Democracy through Law (Venice Commission), *Report on the democratic oversight of the security services*, CDL-AD(2007)016 (2007), Paragraph 73.
6. For example, see Ronnie Kasrils, "To spy or not to spy? Intelligence and democracy in South Africa," in *To spy or not to spy? Intelligence and democracy in South Africa*, ed. Lauren Hutton (Pretoria: Institute for Security Studies, 2009), pp. 9–20.
7. For example, see United States, Department of Defense, "Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO))," Directive No. 5148.11, 21 May 2004.
8. Bulgaria, Law on State Agency for National Security, 40th Session of the National Assembly, Article 88.
9. Bosnia and Herzegovina, Law on the Intelligence and Security Agency, 22 March 2004, Article 42.
10. South Africa, Ministerial Review Commission on Intelligence, *Intelligence in a Constitutional Democracy: Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP* (10 September 2008), p. 77.
11. In the Netherlands, ministerial responsibility was anchored in the constitution as early as 1848; see A. D. Belinfante, *Beginselen van Nederlands Staatsrecht* [Principles of Dutch Constitutional Law] (Alphen aan de Rijn: Samson Publishers, 1981), pp. 64–66.
12. Christian Heyer, "Parliamentary Oversight of Intelligence: The German Approach," in *Intelligence and Human Rights in the Era of Global Terrorism*, ed. Steve Tsang (Westport, CT: Praeger Security International, 2007), p. 69.
13. Council of Europe, European Commission for Democracy through Law (Venice Commission), *Report on the democratic oversight of the security services*, CDL-AD(2007)016 (2007), Paragraph 78.
14. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (McDonald Commission), *First Report: Security and Information* (October 9, 1979), p. 425.
15. Some states make use of a hybrid form of oversight body whose members include both independent experts and former members of parliament.
16. See United Kingdom, Intelligence and Security Committee, *Annual Report 2001–2002*, CM 5542 (2002), pp. 46–50.
17. For more detailed information, see Australia, Inspector-General of Intelligence and Security Act 1986, Act No. 101 of 1986 as amended; and the Inspector General of Intelligence and Security web site (available at http://www.igis.gov.au/).
18. Ian Leigh, "National courts and international intelligence cooperation," in *International intelligence cooperation and accountability*, eds. Hans Born, Ian Leigh, and Aidan Wills (London: Routledge, 2011), p. 232.
19. Frederic Manget, "Another system of oversight: intelligence and the rise of judicial intervention," in *Strategic intelligence: A window into a secret world*, eds. Loch Johnson and James Wirtz (Los Angeles: Roxbury, 2004), pp. 407–409.
20. Ian Leigh, "National courts and international intelligence cooperation," in *International intelligence cooperation and accountability*, eds. Hans Born, Ian Leigh, and Aidan Wills (London: Routledge, 2011), p. 232.
21. The Netherlands, Act of 7 February 2002, providing for rules relating to the intelligence and security services and amendment of several acts (Intelligence and Security Services Act 2002), Article 83, Paragraph 1, p. 31.
22. Ibid., Article 84, Paragraph 1, p. 31.
23. Dana Priest and William M. Arkin, "Top Secret America: A Washington Post Investigation," *The Washington Post*, four-part article series, July–December 2010 (available at http://projects.washingtonpost.com/top-secret-america/; accessed 18 November 2011).
24. The Netherlands, Review Committee on the Intelligence and Security Services (CTIVD), *Annual Report: 2010–2011*, pp. 8–9.
25. Norway, The Act relating to the Monitoring of Intelligence, Surveillance and Security Services, Act No. 7 of 3 February 1995, Section 2.
26. Ibid., Section 2.
27. Ibid., Section 8, Paragraph 2.
28. Commission of Inquiry into the Actions of

Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (2006), p. 17.

29. Ibid., p. 17.
30. Although complaints typically concern events that have transpired, it is worth noting that they sometimes also involve operations that are ongoing or never went beyond the planning stage.
31. Stuart Farson, "The Noble Lie Revisited: Parliament's Five-Year Review of the CSIS Act: Instrument of Change or Weak Link in the Chain of Accountability?" in *Accountability for Criminal Justice: Selected Essays*, ed. Philip C. Stenning (Toronto: University of Toronto Press, 1995).
32. Cyrille Fijnaut, *Het Toezicht op de Inlichtingen- en Veiligheidsdiensten: de noodzaak van krachtiger samenspel* [The oversight of security and intelligence services: the need for closer cooperation] (The Hague, April 2012) (in Dutch).
33. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: 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*, United Nations Document A/HRC/14/46 (17 May 2010).

TOOL 2

TWO

Establishing Effective Intelligence Oversight Systems

Stuart Farson

2

Establishing Effective Intelligence Oversight Systems

Stuart Farson

1. INTRODUCTION

This tool examines one of the major topics of security sector reform: the establishment of effective intelligence oversight and accountability mechanisms (particularly legislative mechanisms) in transition states. An immediate question is: are the mechanisms used by established democracies appropriate models for states still in the process of developing and extending modes of democratic governance? The answer depends on the characteristics of the transition state with relevant considerations including the work that its intelligence services are asked to perform, the scope and scale of the services' activities, and the specific threat environments in which the states exist. In analyzing these factors, one must also take into account broader issues, especially the degree to which the state has developed a democratic political culture and incorporated recognized democratic practices.

Placing the institutions of government under democratic control and making them accountable is one of the most important tasks of democracy. Democratic states vary, however, in how they accomplish this. Some rely on the parliaments to hold the government accountable; others have a more blended system, incorporating a variety of expert bodies. The effectiveness of this process, commonly called oversight, depends not only on the power emanating from legal and constitutional rules determining what may be scrutinized where, when, and how often, but also on the extent to which information is

made available to oversight bodies. Without the ability to obtain knowledge and maintain an institutional memory, no oversight body can develop the expertise it needs to know where to look and what questions to ask in order to accomplish its goals.

Independent institutions such as the Geneva Centre for the Democratic Control of Armed Forces have done much in recent years to develop legal standards and best practices for security sector reform, particularly with regard to intelligence oversight.[1] At the same time, scholars, in addition to producing studies of individual oversight bodies, have attempted to analyze intelligence functions and oversight from a comparative perspective.[2] Yet, largely missing are studies that attempt to discern the effectiveness of oversight models longitudinally.[3] In this regard, only studies of British and American examples have been published.[4]

The limited number of oversight-effectiveness studies is a restricting factor when it comes to recommending one oversight institution over another. First, examinations of oversight systems that do not include longitudinal evaluations have limited comparative value (the value that they do offer likely lies in the problems they discover with the oversight approaches they study). Second, the US and UK oversight systems that have been studied longitudinally may not be the best models for transition states. In the case of the United States, for example, the scope and scale of its intelligence apparatus, the large budgets, and the extent to which the private sector is involved make an examination of US intelligence oversight of modest value to a transition state, whose circumstances are altogether different.

Drawing distinctions among various forms of democratic governance, the next section of this tool considers the nature of transition states. The third section discusses the characteristics of effective oversight. The fourth section identifies several institutional approaches to oversight that have been developed in various states, calling attention to their advantages and disadvantages. The fifth section analyzes the impediments to effective oversight, while the sixth section discusses the legal mandates that oversight bodies require in order to function. Finally, the tool concludes with several key recommendations.

2. TRANSITION STATES

States in the process of developing democratic modes of governance are frequently referred to as transition states. They all share the common experience of democratization, but they may have little else in common, differing not only in their starting points but also in the form of democracy they choose. Some may have been democratic states at one time before experiencing a totalitarian interlude; some may be newly established states, created as the result of the disintegration of a larger state; and some may have experienced tribal domination, deep ethnic divisions, or even civil war. Depending in part on their various histories, the directions that their democracies take will differ. Some will create a unitary state; others, a federalist state. Some will establish a presidency with clear checks and balances on executive power; others will choose a parliamentary system that fuses together the legislative and executive branches of government. Some will be constitutional monarchies; others will be republics. Some will have first-past-the-post electoral systems; others, a form of proportional representation. Some will have unicameral legislatures; others, bicameral legislatures. In addition, their judicial systems

will frequently differ. Taken together, the choices that each transition state makes will have a direct impact on the type of political culture it develops.

The political culture of a democratic state, especially the degree to which democratic ideals are accepted by the public, determines the ways in which those ideals are put into practice. Members of the executive branch in one state, for example, may be more willing to account publicly for their actions than members of the executive branch in another state. So, too, will the development of legislative accountability vary from state to state. Affecting this progress toward democratic governance in many cases will be a movement toward de-democratization[5]—fuelled by the lingering inclination of those in power to use the tools of the state to maintain their power and, more generally, by corruption.

Even the terminology of democratic governance can vary from country to country, particularly when used in the specific context of intelligence oversight. *Accountability*, for example, is generally understood to mean the process of providing an account; more loosely, it implies transparency. Yet in the Commonwealth states that follow the Westminster model, *accountability* also refers to a specific constitutional obligation on the part of responsible cabinet ministers to provide truthful accounts in and to the parliament of the actions (or inactions) of the organizations in their respective ministerial portfolios. Other terms with variable meanings include *threats*, *risks*, *national security*, *independence*, *discretion*, *competence*, *security*, *intelligence*, and *oversight* itself.

3. EFFECTIVE OVERSIGHT

Any legislature, before establishing an intelligence oversight system, would want to judge whether that system was likely to be effective. With so much new literature on the subject now available, one might think this an easy task. However, some words of caution are in order. Although a few scholars have recently published informative studies describing the functions of particular oversight bodies, very few have examined the effectiveness of these bodies in a detailed enough manner and over a long enough period of time to draw meaningful conclusions. (Unfortunately, the studies that did consider a long enough period of time failed to develop useful criteria for judging effectiveness.)

What muddies the water even further is the tendency of executive and legislative branches of government to pursue differing oversight goals. As a result, many democratic countries have developed a blended system in which multiple oversight bodies embrace a variety of purposes through corresponding forms of scrutiny. In such a system, legislative committees may exist alongside expert oversight bodies, sometimes acting in coordination and sometimes not.

Whatever system exists, it is important that legislators be informed about the activities of oversight bodies, that they receive the information in a timely manner, and that the reports of such bodies be readily accessible—which has not always been the case. Most important, legislators need to remain mindful of the objectives to be accomplished through intelligence oversight; otherwise, they can become mired in approaches that are more symbolic than real.[6] That goal is arguably a simple one, the same as for any other government agency. It is not to control the workings of the intelligence services[7] but to hold them and the executive to account in the legislature for their actions and inactions

in a way that the public can see and understand. That being said, however, elements of control may result from at least two of a parliament's major responsibilities—to consider and subsequently approve the release of public funds to cover the cost of an intelligence service's activities, and to adopt or amend legislation governing these services.

In fulfilling their oversight responsibilities, legislators need to evaluate their capabilities, propensities, and limitations. Shortages of time, limited expertise, and insufficient resources all affect what can realistically be achieved. Therefore, legislators need to think hard about what they want to achieve and how that might be accomplished within the parliamentary work cycle. Perhaps an expert oversight body might be more suitable for certain oversight tasks. If so, what would the parliament's relationship with that body be?

In very general terms, parliaments need to be involved with intelligence oversight in two particular ways: one involving compliance, the other relating to efficacy. Specifically, parliaments need to ensure that intelligence services and their contractors do not breach the law, service regulations, or government policy. They also need to ensure that public funds are used properly and effectively.

All too often, parliamentarians assume that their primary responsibility is to conduct ex post facto review of intelligence service activity—that is, to perform their scrutiny after the fact. This is only partially correct. Although much scrutiny can and should take place only after the fact, parliamentarians nevertheless have a responsibility to perform some scrutiny before intelligence operations take place and while they are taking place. For example, parliamentarians have a responsibility to ensure that necessary rules and government policies are in place before operations occur. Similarly, although efficacy can be judged only after the fact, capability and performance criteria need to be evaluated beforehand and on an ongoing basis.

4. APPROACHES TO OVERSIGHT

This section analyzes three approaches to oversight that are currently in practice across a range of democratic states. They are, respectively:

- the legislative committees approach
- the inspectors general approach
- the expert oversight bodies approach

Here, the term *legislative committee* is used generically to include not only parliamentary committees but also committees of legislatures that do not refer to themselves as parliaments.

4.1 LEGISLATIVE COMMITTEES

Legislative committees vary in their types and capacities. In some countries, such as those following the Westminster model, legislative committees can reflect a degree of fusion or overlap between the elected memberships of the legislative and executive branches of government. In other countries, no overlap exists at all.[8]

An important distinction needs to be made at the outset between the legislative committees that exist in congressional systems and those found in parliamentary democracies. Of central importance is the difference in approaches to accountability. In the United States, where the separation of powers encourages each branch of government to provide a check on the others, Congress alone decides what information it will receive and what matters it will consider in testimony before its committees. The powers to appropriate public funds and enact legislation, granted exclusively to Congress, ensure that, with a few notable exceptions, its will is respected. Thus, US congressional committees regularly hear testimony from a full range of senior executive officials, including the administrative heads of the intelligence services, who are expected to respond fully to questions of policy and administration. (The elected members of the US executive branch—that is, the president and vice president—do not testify before Congress.)

By contrast, in most parliamentary systems, the executive branch has the final say over what classified information will be shared with legislative committees simply because the party in power by definition controls the parliamentary majority. There is also a marked difference in expectation regarding who will appear before committees and on what subjects they will respond to questions. In some parliamentary jurisdictions, elected members of the executive branch appear before legislative committees to respond to matters of policy, while other executive officials appear at their discretion to speak to matters of administration.

4.1.1 Congressional approaches in the United States and Brazil

In the United States, as a result of the Church and Pike Committee investigations of the 1970s, Congress decided to establish permanent intelligence committees in both the House of Representatives and the Senate. These committees were tasked with scrutinizing all US intelligence activity, considering its propriety as well as its efficacy. Meeting in secure locations and aided by extensive, security-cleared staffs, these committees are empowered to conduct their oversight before, during, or after the fact. The responsibility for scrutinizing US domestic intelligence activity now also lies with the congressional committees that oversee the work of the Justice Department and the Department of Homeland Security. Committee staff, appointed by both the majority and minority parties, provide a range of services to their respective party members. These are supplemented by the services available from such important congressional support agencies as the Congressional Research Service and the Government Accountability Office.

Brazil provides another example of a congressional system, having recently made the transition from military rule to a federal democracy. For at least a decade after its 1985 transition, the attention of Brazil's new executive branch was dominated by such pressing issues as the economy and the country's large foreign debt. These preoccupations, along with the widespread perception that Brazil had no foreign enemies, produced a lack of urgency with regard to reform of the intelligence sector.[9] More recently, however, the Brazilian Congress has not only revamped the system but also established a series of congressional commissions designed to control the intelligence services. In 1999, it established what is now called the Joint Commission for the Control of Intelligence Activities (CCAI). It has since established four more commissions—including defence commissions in both the House of Representatives and the Senate; the Commission of Public Security against Organized Crime in the House of Representatives; and the permanent sub-commission on public security of the Senate Commission of Constitution, Justice, and Citizenship. All

have been successful in providing a greater degree of transparency—although the CCAI suffered in its early years from a lack of interest among members of Congress, a failure to agree on the commission's internal rules, and an undersupply of technical resources and support personnel.[10]

4.1.2 Parliamentary approaches

Parliamentary approaches to intelligence oversight differ not only from the congressional approach but also among themselves.[11] The key distinctions concern access to classified information, the availability of staff and other resources, the mandate of the committee, and how its members are appointed.

There are no fewer than five approaches to intelligence oversight currently being practiced by parliaments:

- parliamentary committees outside the secrecy loop
- statutory committees of parliamentarians
- permanent statutory parliamentary committees
- special statutory review committees
- blended committees and systems

Parliamentary committees outside the secrecy loop

In some parliamentary democracies (such as Canada and Ireland), the executive branch makes no special provision for parliamentary committees to view classified information. Thus, any person inside the secrecy loop—that is, cleared to handle classified information—would likely be committing a criminal offence should he or she "leak" such information to a member of parliament. As a result, parliamentary committees in these democracies have to operate without any "inside" knowledge of intelligence affairs. Yet they are not entirely impotent. Because they still have the full investigatory powers and resources of the parliament available to them, they can conduct useful scrutiny and bring important issues to the government's attention.[12]

Two further caveats should be noted with regard to this approach: First, there are certainly issues that cannot be adequately covered. For example, where expert oversight bodies raise specific issues of concern, parliament cannot be easily alerted to them. Second, without a dedicated mandate the selection of issues that do receive coverage will be rather unsystematic. As leadership of the committee changes, so will its agenda, practices, and institutional memory.

Statutory committees of parliamentarians

A second approach, practiced by the United Kingdom, involves a statutory committee of parliamentarians.[13] Created by legislation rather than by parliamentary prerogative, the UK Intelligence and Security Committee (ISC) is made up of members of parliament from the House of Commons and the House of Lords—selected not by the political parties, as is the case with parliamentary committees, but by the prime minister, to whom the ISC reports. The reason is that the ISC is not actually a parliamentary committee. It lacks, for instance, the investigatory powers of a parliamentary committee and cannot draw on the usual parliamentary resources and privileges. It is, rather, a committee of parliamentarians.

Its key advantage is that it operates within the secrecy loop, meeting in a secure environment with a security-cleared staff. Another advantage is continuity. Members of the committee drawn from the House of Lords need not, unlike their colleagues in the House of Commons, seek re-election; thus, they offer the possibility for greater continuity and the development of an institutional memory.

On the other hand, the ISC's statutory mandate is limited, encompassing only the expenditures, administration, and policies of the key intelligence services. Also limited are its investigatory resources. Although recently enhanced, they continue to be less than desirable. Consequently, the UK approach tends to discourage the continuous monitoring of events that is, arguably, an important aspect of oversight.

Efforts to bring the ISC under parliamentary control have so far failed, but the role of the political parties has increased. They now strongly influence the selection of ISC members, and parliamentary time is regularly set aside for discussion of redacted (public) versions of ISC reports.[14]

Permanent statutory parliamentary committees

Permanent statutory parliamentary committees on intelligence differ from the British approach in that they are indeed parliamentary committees. Their members are appointed by the political parties, and they can draw on parliamentary resources as needed.

Unlike the ISC, whose staff serves at the pleasure of the executive, a permanent parliamentary committee can largely determine its own course of action, not only in terms of what staff it hires (as long as they are security cleared) but also where it meets (as long as the location is secure).

Membership requirements vary from country to country. In South Africa, for example, proportional representation is the rule, and all of the major political parties must be represented on the committee. In New Zealand, the prime minister and the leader of the opposition must both be members. In Australia, the committee must draw members from both houses of the federal parliament.

The legislation establishing these permanent parliamentary committees normally specifies which organizations they can scrutinize. Although particular activities are sometimes excluded, the remits can be quite broad. In Australia, for example, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) is mandated to scrutinize all of the country's major intelligence organizations, though the list of the activities the committee cannot review is also quite long (see Box 1).

Box 1: Limits to the mandate of the Australian Parliamentary Joint Committee on Intelligence and Security

The functions of the Committee do not include:

a. reviewing the intelligence gathering and assessment priorities of Australian Security Intelligence Organisation (ASIO), Australian Secret Intelligence Service (ASIS), Defence Imagery and Geospatial Organisation (DIGO), Defence Intelligence Organisation (DIO), Defence Signals Directorate (DSD) or Office of National Assessments (ONA); or
b. reviewing the sources of information, other operational assistance or operational methods available to ASIO, ASIS, DIGO, DIO, DSD or ONA; or
c. reviewing particular operations that have been, are being or are proposed to be undertaken by ASIO, ASIS, DIGO, DIO or DSD; or
d. reviewing information provided by, or by an agency of, a foreign government where that government does not consent to the disclosure of the information; or
e. reviewing an aspect of the activities of ASIO, ASIS, DIGO, DIO, DSD or ONA that does not affect an Australian; or
f. reviewing the rules made under Section 15 this Act; or
g. conducting inquiries into individual complaints about the activities of ASIO, ASIS, DIGO DIO, DSD or ONA; or
h. reviewing the content of, or conclusions reached in, assessments or reports made by DIO or ONA, or reviewing sources of information on which such assessments or reports are based; or
i. reviewing the coordination and evaluation activities undertaken by ONA.[15]

A significant difference between statutory committees of parliamentarians and permanent statutory parliamentary committees is their powers and privileges. The latter can hold in contempt parties who do not comply with committee requests, particularly requests for the production of documents and records. In addition, the Australian legislation specifically recognizes that either house of parliament can refer "any matter" concerning the major intelligence services to the PJCIS for review.[16]

Special statutory review committees

At least one jurisdiction (Canada) has obligated future parliaments to establish statutory review committees tasked with scrutinizing intelligence legislation once that legislation has been in operation for several years. The adoption in 1984 of the Canadian Security Intelligence Service Act and the Security Offences Act specifically required the parliament to establish a committee to review these acts after they had been in existence for five years.[17] The Canadian Anti-Terrorism Act adopted in 2001 similarly obligated the parliament to create a review committee after three years.[18] In each case, the committee's mandate was to review the provisions and operation of the law and to include in its report to the parliament recommendations for any changes it considered necessary.

The committees, which were of an ad hoc nature, had a fixed one-year term in which to report. Because they were not perceived to be inside the secrecy loop, they received little support from the expert oversight bodies also established by these statutes.[19]

Blended committees and systems

A number of countries have established blended committees whose members include both

members of the legislature and individuals who are members of neither the executive nor the legislature.

Sweden's Commission on Security and Integrity Protection

In Sweden, for example, the chair and vice chair of the Commission on Security and Integrity Protection (SAKINT) must have served as judges or have equivalent legal experience. The remaining members of the committee, up to a maximum of ten, are appointed from among the nominees proposed by the party groups in the Swedish parliament (the Riksdag)—they may or may not be sitting members of parliament.

The SAKINT has two main responsibilities: to supervise the use of secret surveillance, assumed identities, and associated special investigatory techniques by crime-fighting agencies; and to supervise the processing of personal data by the Swedish Security Service. The SAKINT fulfills these responsibilities primarily through inspections, the purpose of which is to ensure compliance with Swedish laws and regulations.

In conducting its activities, the SAKINT is supported by a staff headed up by a government-appointed director. The legislation that established the SAKINT empowered the committee to obtain information and assistance from the administrative bodies subject to its supervision. The committee may also obtain information from bodies not subject to its supervision. The SAKINT is responsible for reporting to the government annually. There is no such obligation with regard to the Riksdag.

Germany's Blended System

In Germany, the intelligence oversight system is similarly blended. Some have called it "multilateral" because it is comprised of several bodies that operate side by side.[20] The main body is the Parliamentary Control Panel (PKG), the permanent intelligence oversight panel of the lower house of the German parliament (Bundestag). By law, the PKG must meet at least once each quarter. Although membership in the PKG reflects the party composition of the Bundestag, the position of chair alternates annually between a member of the parliamentary majority and a member of the opposition. The members of the committee are assisted in their work by a seven-member secretariat. They focus on the activities of the three federal intelligence services and deliberate in camera. The committee can summon intelligence personnel to testify, obtain documents as necessary, and enter service premises at any time. It must report to the Bundestag in the middle of and at the end of each electoral term.

A second body is the Confidential Committee, which is responsible for scrutinizing the intelligence service budgets (the total amounts of which are communicated to the Bundestag's Budget Committee for inclusion in its budget recommendations). Significantly, the PKG and Confidential Committee sometimes hold joint meetings when budgetary matters are being discussed. (See Wills—Tool 8 for further information).

The final component of the German blended system is the G10 Commission—an independent, quasi-judicial body whose decisions are binding on the intelligence services and the government. The four members of the G10 Commission, chosen by the PKG, may be members of the Bundestag but need not be.

The G10 Commission was initially established to authorise and supervise the interception of mail and telecommunications by the intelligence services. However, when amendments

to the Counter-Terrorism Act adopted in 2007 gave new powers to the intelligence services, the role of the G10 Commission also changed. Now, intelligence services are required to obtain prior approval from the G10 Commission before they can request data from telecommunication service providers that would reveal the location of an activated cell phone, serial numbers, or card codes.

4.2 INSPECTORS GENERAL

This section examines three different approaches to the establishment of inspectors general (IGs) through legislation.[21] The first, developed in the United States, has since served as a model for the other two. They nevertheless vary considerably with regard to who employs the IG, to whom the IG reports, and what topics those reports concern. The practical experiences of the various IGs have also varied, with some enjoying greater access to key personnel and required information than others.

4.2.1 The Inspector General of the US Central Intelligence Agency

Although the Inspector General Act of 1978 required all major departments of the US government to have IGs, it did not apply to the Central Intelligence Agency, which already had its own dedicated IG. First established in 1952, the IG-CIA was in 1978 still appointed by the director of the agency and, in the opinion of many, insufficiently independent. Not until 1989 was the IG-CIA finally given a statutory basis and greater independence. The IG-CIA remains an employee of the CIA and continues to report to the director, but the position is now filled by a presidential nominee who is confirmed by the Senate and can be removed only by the president.

The role of the IG-CIA is primarily to promote economy, efficiency, effectiveness, and accountability within the CIA. He or she does this by conducting independent audits, inspections, investigations, and reviews of CIA programmes and operations. The IG-CIA is also responsible for detecting and deterring fraud, waste, abuse, and mismanagement. With regard to reporting, the IG-CIA is required to communicate his or her findings and recommendations expeditiously to the agency director and to the congressional intelligence committees. When a finding concerns alleged violations of the law, the IG-CIA must also inform the attorney general.[22]

4.2.2 The Inspector General of the Canadian Security Intelligence Service

Unlike the IG-CIA, who is an employee of the agency he or she oversees, the person occupying the Office of the Inspector General of the Canadian Security Intelligence Service (OIG-CSIS) is not an employee of the service but of the Department of Public Safety, appointed by the cabinet and reporting to the Deputy Minister of Public Safety. The mandate of the OIG-CSIS, created under the Canadian Security Intelligence Service Act of 1984, is much more limited than that of the IG-CIA. It focuses entirely on compliance with Canadian laws, regulations, and policies. Every twelve months, the OIG-CSIS must review the report submitted by the CSIS director to the responsible minister concerning the service's operational activities. The OIG-CSIS has to certify the report, identifying any activities that are not authorized by the CSIS Act or in contravention of directions issued by the minister. In addition, the OIG-CSIS must identify any activities that involve an unreasonable or unnecessary use of CSIS powers.

Governing law specifically entitles the OIG-CSIS to receive from the CSIS director and other CSIS employees whatever information, reports, and explanations it considers necessary for the performance of its duties. In practice, however, IGs have had difficulty meeting with CSIS directors.

The OIG-CSIS does not communicate directly with the parliament, even regarding matters of non-compliance. In fact, members of parliament can learn this information in only three ways: if the responsible minister voluntarily chooses to inform them; if they obtain the information through an Access to Information Act request; or if the information is included in one of the annual reports prepared by the Security Intelligence Review Committee (SIRC), an expert body that operates well outside the executive branch (see Section 4.3 below).[23]

4.2.3 The Australian Inspector General of Intelligence and Security

The Australian Inspector General of Intelligence and Security (AIGIS) is similar to its US and Canadian counterparts in that it has a statutory basis. Established in 1986 by the Inspector General of Intelligence and Security Act, the office is not part of any department or agency. Instead, it exists independently within the prime minister's own portfolio.

The AIGIS, who is appointed by the governor general, has a much broader remit than the US and Canadian IGs. Instead of scrutinizing just one service, he or she has responsibility for the entire Australian intelligence community. Although the AIGIS to a degree performs different functions for different services, his or her main duties are fourfold:

1. monitoring compliance with the laws, directions, and guidelines that govern the activities of the various services
2. evaluating the propriety of those activities
3. evaluating the effectiveness of those activities
4. determining whether any of those activities is inconsistent with or contrary to a human right

Perhaps not surprisingly, the AIGIS has traditionally focused most of his or her investigative resources on the affairs of the Australian Security Intelligence Organisation (ASIO)—the reason being that the jurisdiction of the ASIO is primarily domestic, and it is thus more likely to infringe on the rights of Australian citizens and residents than the country's foreign and defence intelligence services. (A recent estimate suggests that 60 to 70 percent of AIGIS resources are spent on proactive inspection programmes.[24]) When conducting a full inquiry, the AIGIS can and does use the same powers of investigation provided to royal commissions of inquiry. That is, the AIGIS can compel witnesses to appear at hearings and testify truthfully. He or she also has the power to compel the production of documents and to enter service premises. Meanwhile, the AIGIS's security of tenure is assured by the fact that he or she can be removed only for cause.

Governing law requires the AIGIS to submit an annual report of his or her activities to the prime minister, who must table the report in both houses of the parliament. Although former holders of the office generally do not view the AIGIS as an oversight body with the capacity to effect change,[25] the recommendations that the office produces are nevertheless taken seriously by the intelligence services and their respective ministers.[26]

It should be noted finally that, in addition to review by the AIGIS and the PJCIS (discussed above), the intelligence services of Australia are also scrutinized by the Australian National Audit Office.

4.3 EXPERT OVERSIGHT BODIES

Expert oversight bodies are normally established by statute. Their distinguishing characteristics include the functions they perform, their degree of independence from the executive and the parliament, to whom they report, how their members are selected, and whether or not there are any membership requirements.

4.3.1 Canada's Security Intelligence Review Committee and Office of the Communications Security Establishment Commissioner

Canada has two such expert oversight bodies: the SIRC and the Office of the Communications Security Establishment Commissioner Canada (OCSEC). The SIRC, which operates outside both the executive and legislative branches of government, has a maximum of five members, all of whom must be privy councillors and therefore under an oath of secrecy. In addition, no member of the SIRC may be currently a member of parliament.[27] Originally, it was hoped that its membership would be drawn from persons who had experience as privy councillors through having served as responsible ministers. This has not always been the case. The SIRC meets in a secure environment and has a security-cleared staff. Beyond receiving the OIG-CSIS's certificate of compliance, the SIRC has a mandate of its own to ensure CSIS compliance, including the power to investigate complaints against the service (see Box 2). In this regard, it can instruct the OIG-CSIS or the service itself to conduct a review of specific activities.

Box 2: The mandate of the Canadian Security Intelligence Review Committee

The functions of the Review Committee are:

a. to review generally the performance by the Service of its duties and functions and, in connection therewith,
   i. to review the reports of the Director and certificates of the Inspector General transmitted to it pursuant to subsection 33(3),
   ii. to review directions issued by the Minister under subsection 6(2),
   iii. to review arrangements entered into by the Service pursuant to subsections 13(2) and (3) and 17(1) and to monitor the provision of information and intelligence pursuant to those arrangements,
   iv. to review any report or comment given to it pursuant to subsection 20(4),
   v. to monitor any request referred to in paragraph 16(3)(a) made to the Service,
   vi. to review the regulations, and
   vii. to compile and analyse statistics on the operational activities of the Service;
b. to arrange for reviews to be conducted, or to conduct reviews, pursuant to section 40; and
c. to conduct investigations in relation to
   i. complaints made to the Committee under sections 41 and 42,
   ii. reports made to the Committee pursuant to section 19 of the Citizenship Act, and
   iii. matters referred to the Committee pursuant to section 45 of the Canadian Human Rights Act.[28]

In conducting its reviews, the SIRC has the right to access any information under the control of the OIG-CSIS or the CSIS that the SIRC deems necessary to the performance of its duties and functions—including reports and explanations. The SIRC may submit reports to the responsible minister at its discretion; however, it must always submit an annual report that the responsible minister can table in parliament. Although the SIRC may otherwise determine its contents, the annual report may not disclose classified information.

It was originally hoped that the SIRC's annual report would provide the parliament with the information it needed to conduct effective intelligence oversight. In practice, however, the SIRC has not always been forthcoming.[29]

When the Special Committee of the House of Commons on the Review of the CSIS Act and Security Offences Act (see Section 4.1.2 above) met to consider the respective roles of the SIRC and the OIG-CSIS, its members were at a loss to understand why the functions of the OIG-CSIS could not be folded into those of the SIRC. The responsible minister at the time fought hard to convince the special committee of the OIG-CSIS's importance and the need for both bodies. As a consequence, the special committee changed course and refrained from recommending that the OIG-CSIS be disbanded. Years later, however, a subsequent government accepted the incumbent's resignation and then left the office vacant for more than a year. Very recently the government has indicated that it now intends to collapse the role of the OIG-CSIS into SIRC. While ostensibly suggesting that it was doing this to cut administrative costs, it also argued that oversight would be improved.[30]

Until 1996, when an executive order established the OCSEC, the Communications Security Establishment (CSE), Canada's signals intelligence service, had no external oversight. Five years later, as part of an omnibus Criminal Code bill, the parliament adopted the Anti-Terrorism Act, which gave a statutory basis to both the OCSEC and the CSE (which, like the CSEC, had been operating under an executive order). The Anti-Terrorism Act gave the OCSEC a limited mandate to ensure that the CSE operates in compliance with Canadian law. The OCSEC is also empowered to hear complaints against the agency. The requirements for office include experience as a senior court judge. Once in office, the OCSEC can be dismissed only for cause.

Like the OIG-CSIS and the SIRC, the OCSEC operates within the loop of secrecy, with secure premises and limited security-cleared staff. In addition, the OCSEC enjoys the same investigatory powers as any commissioner under the Inquiries Act. Like the SIRC, the OCSEC must submit an annual report that the responsible minister can table in parliament.

These two annual reports provide the only information that the Canadian parliament receives directly from the OCSEC and the SIRC. In neither case is the government bound to take action on the report's recommendations.

4.3.2 Belgium's Standing Intelligence Agencies Review Committee

An expert body similar to the SIRC performs intelligence oversight in Belgium. Yet the Belgian Standing Intelligence Agencies Review Committee (known as Committee I) differs from the Canadian example in several important respects. First, its mandate covers two intelligence services (State Security, which is a civilian service; and the General Intelligence and Security Service, the military counterpart of State Security) as well as the Coordination Unit for Threat Assessment.[31] Second, Committee I's mandate extends beyond ensuring

compliance with laws and regulations to consideration of the services' efficiency and the coordination between them. Third, the three members of Committee I—all of whom must be security cleared, hold a degree in law, and have relevant professional experience—are appointed by the Belgian Senate (not, as in Canada, by the cabinet). Finally, the chair of the committee must be a magistrate.

No member of Committee I can be a member of parliament, but the committee's enabling legislation does place an onus on both houses of the parliament to establish permanent committees to monitor the work of Committee I and consider its reports. The law further requires the members of the parliamentary committees to take appropriate security precautions, and it places them under an obligation to keep the information they receive confidential, even after leaving office, under penalty of law.

5. IMPEDIMENTS TO EFFECTIVE OVERSIGHT

In transition states, many factors can impede the establishment of effective intelligence oversight practices. This section discusses the most prevalent impediments.

5.1 RELUCTANCE TO HOLD THE EXECUTIVE BRANCH TO ACCOUNT

The most basic impediment to effective oversight is the reluctance of legislators to enact and make use of measures holding the executive branch to account. In transition states where the executive branch has not been previously held to account, legislators usually have to experiment with a variety of approaches before determining what method works best for them. Relying on committee hearings alone to provide effective oversight will likely prove inadequate. Experience has shown that staff work, research studies, site visits, and in camera hearings will also be required.

5.2 STEEP LEARNING CURVE

Security and intelligence activities differ from most other functions of government in that they affect and/or involve nearly all departments or ministries. Because proper oversight requires a great deal of familiarity with the functions and practices of intelligence services and the complex ways in which they interact with other government agencies, the learning curve is steep and thus difficult for legislators with many other demands on their time and attention. Developing the necessary expertise takes time, especially when one takes into account the general reluctance of intelligence officers to share their detailed knowledge.

5.3 LACK OF TRUST

If intelligence services and intelligence oversight bodies do not trust one another, there can be no frank discussions, no significant exchanges of information, and no effective oversight. To build relationships of trust, external oversight bodies (especially legislative committees) should avoid focusing solely on compliance. Limiting oversight in this way fosters a confrontational, us-against-them environment and discourages intelligence personnel from seeing any benefits to them in the oversight process. Instead, at least in the initial phase, they see only considerable difficulties.

For oversight to be effective, intelligence services need to experience its benefits as well. An emphasis on efficacy, for example, can benefit a service through recommendations that encourage the executive branch to provide the service with greater resources. The service can also experience the benefits of oversight when a legislative committee or expert oversight body corrects a media report wrongly accusing service members of misconduct or questioning their effectiveness.

5.4 DENIAL OF ACCESS TO PERSONS, PLACES, PAPERS, AND RECORDS

The single most important impediment to effective oversight is the denial of access to persons, places, papers, and records. Without such access, oversight bodies cannot function adequately (see also, Nathan–Tool 3). They cannot test whether the information they receive from the executive branch is accurate, nor can they properly develop a line of investigation into a particular matter. Instead, they have to rely solely on what they are told and whatever they can obtain from open sources.

5.5 TIME PRESSURES AND THEIR EFFECT ON SCRUTINY

The time pressure that legislators feel can have an adverse effect on the type of scrutiny they undertake. Studies of US congressional oversight committees have found that legislators, rather than looking for problems on their own, are more likely to take up issues that have already caught the public's attention[32]—and they have good reason for doing so. Because legislators are busy people with many responsibilities (including their own re-election), they tend to pursue those matters most likely to offer them a personal political benefit. The fact that intelligence service scrutiny rarely takes place in public means that it offers them little opportunity for political benefit.

The capacity of legislators to oversee intelligence services is further impeded by the nature of the legislative branch itself. Time available for oversight is limited not only by the work that all legislators must perform but also by the sittings of the legislature. In most jurisdictions, legislative work comes to a halt when the legislature is not in session and during elections. Placing the responsibility for oversight with an expert body offers a partial solution to this problem.

5.6 PARTISANSHIP

The oversight process can all too easily be hampered by partisanship. In the United States, for example, when partisanship becomes excessive, it can thwart opposition efforts to scrutinize an intelligence service by delaying or controlling the work of the congressional oversight committees.[33] Similarly, in most parliamentary jurisdictions, the governing party controls the agendas of all legislative committees through its majority representation. To counteract this dominance, which is the general rule, some jurisdictions require the chair of the intelligence oversight committee to be a member of an opposition party.

Alternating the chair in this way and selecting committee members based on the right balance between government and opposition are important ways in which the partisanship can be minimized and cooperation promoted. In general, oversight functions best when members of oversight committees work together in the collective pursuit of outcomes that serve the national interest.

5.7 DELAYED REPORTS FROM EXPERT OVERSIGHT BODIES

In the event that expert bodies are established to conduct various proactive and routine forms of scrutiny, it is very important that their reports and analyses are made available to legislators in a timely fashion. Regardless of what aspects of intelligence the legislators themselves scrutinize, they still need to be aware of the broadest possible picture in order to carry out such wider responsibilities as appropriating public funds and reviewing existing legislation. If legislators cannot receive reports in a timely manner and cannot question the members of expert bodies about their recommendations, the legislators' ability to meet their own responsibilities will be greatly impaired.

5.8 INADEQUATE RESOURCES

To a great extent, the ability of legislators to carry out effective oversight depends on the resources made available to them. The most important resources in this regard are staff and access. As noted previously, legislators are busy people with a broad range of responsibilities. Without the help of a permanent, highly skilled, non-partisan support staff with a broad knowledge of the intelligence community, legislators are likely to perform oversight that is limited at best, focusing on committee hearings rather than investigative work. Furthermore, to perform effective oversight, legislators also need access to a broad range of information, including research services and audit capabilities.

The creation of a permanent non-partisan support staff can also aid in the development and persistence of an institutional memory. Because intelligence expertise takes so long to develop, the turnover of legislators (which can be considerable in some jurisdictions) often results in a loss of knowledge and experience. For obvious reasons, the presence of a permanent, non-partisan staff alleviates this impediment to effective oversight.

6. DESIGNING LEGAL AND INSTITUTIONAL FRAMEWORKS FOR AN OVERSIGHT SYSTEM

Oversight mandates should be of the widest possible remit. Although the mandate for a particular oversight body should depend largely on its place within the overall oversight system, taken collectively these mandates should cover a wide range of intelligence service issues, from administration and operations to policy and budgeting.

For an oversight system to be effective, it must ensure that the intelligence services it monitors comply with applicable laws, regulations, and policies and that they are effective in the tasks that they perform. Although monitoring compliance can be a relatively simple task, evaluating efficacy is much more complicated because it requires a comprehensive examination of the security and intelligence system as a whole. In this endeavour it is not sufficient merely to scrutinize the agencies that collect intelligence. It is also necessary to examine whether elected leaders are: actively and routinely engaged in determining strategies and responsibilities for the intelligence services; setting intelligence requirements that meet current threats and opportunities; establishing priorities to be followed; and ensuring that the various components of the intelligence system are following these priorities.

If one considers the security and intelligence system as a whole, it seems obvious that, to be helpful in protecting national security, intelligence services must provide the government at any moment with the "best truth" available. However, intelligence work is not a perfect science, and the "best truth" may sometimes be seriously flawed. Such is the nature of the work; nevertheless, it is essential that intelligence services "speak truth to power" without regard to the consequences of failure. To promote and maintain this attitude within the intelligence community, services need the full support of all political parties, fair-minded criticism notwithstanding. The problem is that legislatures are political bodies, where governments-in-waiting routinely seek to show up the party in power by offering alternative positions. Hence, the temptation to seek partisan advantage often trumps the will to cooperate. For this reason, intelligence oversight is often most effective when carried out by expert oversight bodies with no direct connection to either the executive or the legislative branch. This arrangement offers the possibility of removing politics from the work of intelligence oversight.

With regard to intelligence services' compliance with the law, expert oversight bodies should be mandated not only to review service operations after the fact but also to consider on an ongoing basis whether the applicable laws, regulations, and policies are functioning well or need to be revised. These bodies should also be obligated to investigate complaints against services with intrusive or coercive capabilities or to ensure that complaints are fully investigated by competent tribunals (see Forcese—Tool 9). Furthermore, they should be required to submit reports on a regular basis to all relevant authorities; and these reports should contain, where appropriate, recommendations for redress.

With regard to intelligence services' efficacy, expert oversight bodies need to measure both capability and performance. Often, this measuring takes place after the fact (lessons to be learned), but it should also have an ongoing component that considers whether a service's current capabilities are likely to meet the needs that the government foresees for the future. Supreme audit institutions (SAIs) usually have the necessary skills to develop such measurements (see Wills—Tool 8); but because they ordinarily have responsibility for the full range of government operations, they may not be able to devote to the intelligence sector the attention it requires on a regular basis. Consequently, legislatures may find it necessary to grant special dispensations to SAIs or to create new audit bodies to meet this need.

When creating mandates for oversight bodies, legislators need to ensure that the enabling legislation grants overseers sufficient access to all of the components of the security and intelligence infrastructure. Doing so will permit oversight bodies to assess the overall capabilities of the intelligence community. Without such a broad remit, the executive branch can all too easily move around responsibilities to circumvent close scrutiny. A broad remit also allows those who conduct oversight to scrutinize the structural relationships of the organizations involved, how these relationships operate in practice, and how they affect the costs of joint operations.

Furthermore, enabling legislation should grant members of oversight bodies some security of tenure in order to reduce the potential influence of the executive branch on their decision making. That is, organizationally, they may be of the executive branch, but they should not be in it.

So, one might ask, if a legislature creates expert bodies to perform intelligence oversight, what oversight is left for the legislators to perform? The answer relates to the three critical responsibilities that legislatures have in parliamentary democracies:

- to debate and adopt legislation
- to approve the expenditure of public funds by departments and agencies of government
- to hold the government to account for its actions or inaction

All of these responsibilities require that legislators be actively involved with the work of intelligence oversight. If they are to fulfill their obligations with regard to enacting legislation, budgeting, and accountability, the members of legislative committees will need not only timely access to the reports of expert oversight bodies but also the ability to question the members of those bodies about the reports they submit. In addition, legislators will sometimes need to conduct their own investigations when matters have arisen that jeopardize the public's trust in the intelligence services. Legislators will also need to scrutinize at routine intervals the activities of the expert oversight bodies to ensure that they are operating effectively and have appropriate resources.

Finally, as discussed in Section 5.4, without access to persons, places, papers, and records, there can be no effective oversight. Consequently, the most important power of an oversight body is the power to compel access. Although legislatures may possess the right of access in general, legislative committees may be prevented from accessing classified information, personnel, or work environments because terms of such access have not been firmly established in statutory law.

7. RECOMMENDATIONS

Any legislation establishing a system of intelligence oversight should specifically cover the following matters:

The establishment of a legislative committee with guaranteed access to persons, places, papers, and records.

The legislation enabling this committee should specify its powers with regard to access—such as the powers to issue subpoenas, to compel testimony under oath or affirmation, and to enter and search intelligence service premises. It should also specify who may become a member of the committee and what resources the committee will command. Its two purposes, as defined in the legislation, should be to prevent abuses by the security and intelligence services and to improve the effectiveness, efficiency, and economy of their operations. The committee should further be able to instruct any support body to undertake oversight projects that it has neither the competence nor the time to pursue—such projects to be completed and reported on within a reasonable time frame.

The obligations placed on the committee should include a requirement that it conduct its oversight within a secure environment. Its members and staff should all be security cleared and they should be placed under oath not to reveal classified information.[34] In addition, although permitted to issue public reports at its discretion, the committee should be obligated to prepare a report at least once a year that will be tabled in the

legislature and made available to the public. All such reports should be vetted by the services for inappropriate inclusion of classified material, but the final say regarding what subject matter to include should rest with the committee.

The legislation should further stipulate that the committee conduct regular reviews of national security legislation to determine whether the legislation is operating as intended and continues to reflect the current threat and technological environments. It should include specific penalties for committee members and staff who leak information. Finally, it should authorize the members of the committee to establish ad hoc commissions of inquiry when outside expertise is required or an issue is likely to be highly partisan.

The establishment of an independent body to hear complaints against any intelligence service.

Such a body should be the first point of contact for anyone making a complaint against an intelligence service. Its enabling legislation should provide specific protections for whistleblowers. Whistleblowers should be protected provided that they have not revealed classified information that has not previously been made public and that such disclosures were made in good faith. Protections should also apply if disclosures have since been judged to be in the public interest. Furthermore, the body should also have the power to review individual cases after they have been adjudicated to ensure that the whistleblowers have not suffered inappropriate repercussions with regard to their employment.

The establishment of one or more expert oversight bodies to conduct oversight primarily, but not exclusively, of a proactive nature.

These bodies should be able to meet and converse freely with one another and with legislative committees, provided that such meetings take place in secure environments. They may also serve the needs of the executive branch, but their primary purpose should be to assist legislative committees in preventing abuses of power and encouraging greater efficacy. Although these oversight bodies should be able to develop their own work plans and schedules, they should take direction as well from legislative committees and the executive branch. Their scrutiny may take place before, during, or after the events they choose to review.

Endnotes

1. See, for example, Hans Born (ed.), *Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices* (Geneva: DCAF, 2003); and Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Geneva: DCAF, University of Durham, and Parliament of Norway, 2005).
2. For comparative studies, see Jean-Paul Brodeur, Peter Gill, and Dennis Tollborg (eds.), *Democracy, Law, and Security: Internal Security Services in Contemporary Europe* (Aldershot, UK: Ashgate, 2003); Thomas C. Bruneau and Steven C. Boraz (eds.), *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness* (Austin: University of Texas Press, 2007); Stuart Farson, Peter Gill, Mark Phythian, and Shlomo Shpiro (eds.), *PSI Handbook of Global Security and Intelligence: National Approaches*, (Westport, CT: Praeger Security International, 2008); Greg Hannah, Kevin O'Brien, and Andrew Rathmell, *Intelligence and Security Legislation for Security Sector Reform*, Technical Report TR-288-SSDAT (RAND Europe, 2005).
3. A few studies have looked at the effectiveness of particular oversight bodies over a specific period of time. These include: Stuart Farson, "The Noble Lie Revisited: Parliament's Five-Year Review of the CSIS Act: Instrument of Change or Weak Link in the Chain of Accountability?" in *Accountability for Criminal Justice: Selected Essays*, ed. Philip C. Stenning (Toronto: University of Toronto Press, 1995), pp. 185–212; Loch Johnson, *A Season of Inquiry: The Senate Intelligence Investigation* (Lexington: University Press of Kentucky, 1985); Kathryn S. Olmsted, *Challenging the Secret Government: The Post-Watergate Investigations of the CIA and FBI* (Chapel Hill: University of North Carolina, 1996); and Kent Roach, "The Parliamentary Review of the Anti-Terrorism Act," *Criminal Law Quarterly* 52 (May 2007), pp. 281–4.
4. Anthony Glees, Philip H.J. Davies, and John L. Morrison, *The Open Side of Secrecy: Britain's Intelligence and Security Committee* (London: Social Affairs Unit, 2006); Frank J. Smist Jr., *Congress Oversees the United States Intelligence Community, 1947–1994, 2nd Edition* (Knoxville: University of Tennessee Press, 1994).
5. See Charles Tilly, *Democracy* (Cambridge: Cambridge University Press, 2007).
6. See Peter Gill, "Symbolic or Real? The Impact of the Canadian Security Intelligence Review Committee, 1984–88," *Intelligence and National Security* 4, No. 3 (1989) pp. 550–575.
7. In parliamentary democracies, control of the intelligence services is normally the responsibility of the executive. However, elements of parliamentary control may result from the parliament's powers to approve intelligence service funding and enact legislation governing the services.
8. In some governmental systems where a separation of powers exists, legislative committees cannot call elected members of the executive branch to testify.
9. See Thomas C. Bruneau, "Intelligence Reforms in Brazil: Contemporary Challenges and the Legacy of the Past," *Strategic Insights* VI, No. 3 (May 2007) (available at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA485122).
10. See Marco Cepik, "Structural Change and Democratic Control of Intelligence in Brazil," in Thomas C. Bruneau and Steven C. Boraz (eds.), *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness* (Austin: University of Texas Press, 2007) pp. 149–169.
11. For a comparative analysis of parliamentary oversight systems in the European Union, see Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (Brussels: European Parliament, 2011), especially the charts on pp. 92–95.
12. The Canadian Senate's Committee on National Security and Defence when chaired by Colin Kenny covered a broad range of subjects and produced several important reports, some based on in camera work.
13. Canada has considered this approach but not yet adopted it.
14. These reports were originally prepared in the Cabinet Office. However, because the Cabinet Office was perceived to have a potential conflict of interest, they are now prepared in a secure environment that is considered more independent.
15. Australia, Intelligence Services Act 2001, Section 29(3).
16. Ibid., Section 29(1)(b).
17. See Canada, Special Committee on the Review of the CSIS Act and the Security Offences Act, In Flux But Not In Crisis (September 1990).
18. See Kent Roach, "The Parliamentary Review of the Anti-Terrorism Act," *Criminal Law Quarterly* 52 (May 2007), pp. 281–4.
19. See Stuart Farson, "The Noble Lie Revisited: Parliament's Five-Year Review of the CSIS Act: Instrument of Change or Weak Link in the Chain of Accountability?" in *Accountability for Criminal Justice: Selected Essays*, ed. Philip C. Stenning (Toronto: University of Toronto Press, 1995), pp.

185–212.

20. See Shlomo Shpiro, "Parliamentary and Administrative Reforms in the Control of Intelligence Services in the European Union," *Columbia Journal of European Law* 4 (1998), pp. 545–578.
21. See Geoffrey R. Weller, "Comparing Western Inspectors General of Intelligence and Security," *International Journal of Intelligence and CounterIntelligence* 9, No. 4 (1996), pp. 383–406.
22. See Frederick M. Kaiser, "The watchers' watchdog: The CIA inspector general," *International Journal of Intelligence and CounterIntelligence* 3, No. 1 (1989), pp. 55–75.
23. For many years, delays in providing OIG-CSIS compliance certificates to the SIRC made it impossible for the committee's annual report to comment on—and thus inform the parliament about—CSIS compliance issues.
24. See Ian Carnell and Neville Bryan, "Watching the watchers: How the Inspector-General of Intelligence and Security helps safeguard the rule of law" (paper presented at the Safeguarding Australia 2005 conference, 12–14 July 2005) (available at http://www.igis.gov.au/public_statments/conference_papers.cfm).
25. In some jurisdictions that follow the Westminster model, members of the executive branch draw a distinction between review and oversight. They use the term *review* to mean mere scrutiny and the term *oversight* to mean scrutiny accompanied by the power to effect change. Thus, in scrutinizing the activities of intelligence services, review bodies could only make recommendations for change, while oversight bodies could compel it.
26. See Ian Carnell and Neville Bryan, "Watching the watchers: How the Inspector-General of Intelligence and Security helps safeguard the rule of law" (paper presented at the Safeguarding Australia 2005 conference, 12–14 July 2005) (available at http://www.igis.gov.au/public_statments/conference_papers.cfm).
27. Originally, it was hoped that the members of the SIRC would be former responsible ministers, but this has not always been the case.
28. Canadian Security Intelligence Service Act, R.S.C., 1985, Chapter C-23, Section 38.
29. See Stuart Farson, "The Noble Lie Revisited: Parliament's Five-Year Review of the CSIS Act: Instrument of Change or Weak Link in the Chain of Accountability?" in *Accountability for Criminal Justice: Selected Essays*, ed. Philip C. Stenning (Toronto: University of Toronto, 1995), pp. 185–212.
30. Bruce Cheadle, "Conservatives use budget bill to cut spy agency inspector general's office," *Canadian Press*, April 26, 2012.
31. Committee I is also responsible for ensuring that information on terrorism and extremism is passed on by the Coordination Unit for Threat Assessment to the relevant political, administrative, and judicial authorities.
32. See, for example, Mathew D. McGubbins and Thomas Schwartz, "Congressional Oversight Overlooked: Police Patrols versus Fire Alarms," *American Journal of Political Science* 28, No. 1 (February 1984), pp. 165–179.
33. Marvin C. Ott, "Partisanship and the Decline of Intelligence Oversight," *International Journal of Intelligence and CounterIntelligence* 16, No. 1 (2003), pp. 69–94.
34. Vetting by the security services of legislators and certain other officeholders (such as judges) can be constitutionally problematic from a separation-of-powers point of view. That is, it is generally inappropriate for a member of the executive branch to decide on the suitability of a member of the legislative or judicial branch. For obvious reasons, some form of vetting is necessary for anyone who will be routinely handling classified information. Fortunately, there are a number of ways around the constitutional problem. The legislature and the judiciary can conduct on their own informal vettings of the sort that take place when a person is appointed to be a minister; alternatively, they can employ outside security firms to conduct more formal vetting processes. Such vetting yields three important benefits: First, intelligence services are more likely to trust and be more forthcoming with oversight bodies whose members have been vetted. Second, foreign partners are more likely to share intelligence if they are assured that the shared information will not be revealed by unvetted oversight bodies. Third, studies of elite deviance reveal that there are "bad apples in every barrel." Judges have been corrupted, members of oversight bodies have been forced to resign over conflicts of interest, and legislators have been found guilty of treason. Vetting can remove these "bad apples" before they cause undue harm.

TOOL 3

Intelligence Transparency, Secrecy, and Oversight in a Democracy

Laurie Nathan

THREE

3

Intelligence Transparency, Secrecy, and Oversight in a Democracy

Laurie Nathan[1]

1. INTRODUCTION

The existence of intelligence services in democratic countries gives rise to a political paradox. On the one hand, the services are established in order to protect the state, citizens and other persons under the state's jurisdiction, and the democratic order; and they are given special powers and capabilities for this purpose. They are usually entitled by legislation to acquire confidential information through surveillance, interception of communication, and other methods that infringe the right to privacy; to undertake covert operations aimed at countering threats to national security; and to operate with a high level of secrecy.

On the other hand, the intelligence services and members of the executive can abuse these powers and capabilities to undermine the security of individuals and subvert the democratic process. They can violate human rights in contravention of the law, interfere in lawful political activities, and favour or prejudice a political party or leader. They can intimidate the opponents of government, create a climate of fear, and fabricate or manipulate intelligence in order to influence government decision making and public opinion. They can also abuse intelligence funds and methods for personal gain.

Given these dangers, democratic countries are confronted by the challenge of constructing rules, controls, and oversight mechanisms aimed at minimizing the potential for illegal

conduct and abuse of power and at ensuring that the intelligence services fulfil their responsibilities in accordance with the constitution and legislation.

These aims apply equally to the control and oversight bodies governing other state organizations, but they are very difficult to achieve in the world of intelligence because of the high level of secrecy surrounding the intelligence services and their operations. The secrecy inhibits monitoring and review by oversight bodies, stifles public scrutiny, and makes it easy for intelligence officers to hide misconduct.

This tool focuses on secrecy, openness, and provision of information in relation to intelligence oversight bodies. These bodies include parliament, a parliamentary intelligence oversight committee, the judiciary, a supreme audit institution (SAI), an independent inspector general of intelligence (as in Australia, New Zealand, and South Africa), and an expert intelligence oversight body (such as the Review Committee on the Intelligence and Security Services in the Netherlands). The tool outlines the political and conceptual debate around intelligence secrecy and transparency; presents good practice regarding legislation on protection of and access to information; and discusses the intelligence information that is required by parliament and other oversight bodies. It concludes with a set of recommendations.

Whereas discussions on intelligence secrecy generally focus on what should be withheld from disclosure, this tool explores in a more positive manner the areas of intelligence that ought to be disclosed in the interests of effective oversight and democratic governance.

It should also be stressed at the outset that excessive secrecy gives rise to suspicion and fear of the intelligence organizations, reducing public support for them. In a democracy, unlike a police state, intelligence agencies must rely on public cooperation rather than coercion and terror to be successful. The provision of greater information about the services would raise their profile in a positive way, reduce the apprehension and fears induced by secrecy, improve cooperation with the services, and thereby boost their effectiveness.

2. THE PROBLEM OF TRANSPARENCY AND SECRECY IN INTELLIGENCE OVERSIGHT

The most important and vexed issue regarding democratic governance of the intelligence services is that of secrecy. It is the most important issue because the higher the level of secrecy, the harder it is to ascertain and assess the features and performance of the services. In the absence of adequate information, it is impossible for oversight bodies to determine and discuss meaningfully the role and orientation of the services, the need for intelligence reform, and the vital question of whether the services are safeguarding or undermining the security and freedom of citizens and other persons under a state's jurisdiction.

The subject is vexed because it is characterized by strong competing pressures. On the one hand, certain aspects of the intelligence community and its activities must be kept secret in order to avoid compromising operations and the lives of intelligence officers and their sources. On the other hand, secrecy is antithetical to democratic governance; it

prevents full accountability; and it provides fertile ground for abuse of power, illegality, and a culture of impunity.

This section explores the debate around intelligence transparency and secrecy and sets out a democratic approach. These issues are of great relevance to parliament. Through its involvement in drafting and approving laws and policies that govern secrecy and access to information, parliament plays a major role in shaping the extent to which the intelligence dispensation is open or closed to public scrutiny. Moreover, parliament is not only responsible for holding the executive and state organs to account, it is itself accountable to the public and is obliged to provide citizens with information about the intelligence community. Parliamentary debates on intelligence laws, policies, and budgets should therefore be held in open session.

2.1 MOTIVATIONS FOR INTELLIGENCE SECRECY

Secrecy is an intrinsic and necessary feature of intelligence services because of the nature of their mandate and functions. The services are concerned with conventional and non-conventional threats to national security; with hostile countries and terrorist and criminal organizations; with the physical protection of government leaders and state installations; and with the protection of classified state information. Secrecy gives the intelligence services a competitive advantage in tackling these concerns, and extreme transparency would put them at a distinct and dangerous disadvantage.

More specifically, secrecy is necessary for the following purposes:

- to prevent the targets of intelligence operations from becoming aware that they are under surveillance.
- to prevent targets and adversaries from learning about the methods used by services.
- to protect the lives of intelligence officers and informants.
- to ensure the safety of the very important persons (VIPs) who are under the protection of the intelligence services.
- to maintain the confidentiality of information provided by foreign intelligence services.
- to avoid being compromised in various ways by rival intelligence services.

While these requirements for secrecy are reasonable, intelligence services tend to have an excessive and sometimes obsessive attitude towards secrecy. They argue that transparency in non-sensitive areas will lead inexorably to openness in sensitive areas, with dire results. They consequently develop internal systems, procedures, and rules that do not permit for any laxity or flexibility in relation to secrecy. It is also the case that the services might prize secrecy because it gives them a certain mystique and elite status.

Intelligence services are sometimes reluctant to disclose information even to parliamentary oversight bodies that are authorized to receive intelligence. The services claim that because the parliamentarians are not trained and disciplined in terms of maintaining confidentiality, there is a risk that they will reveal sensitive information to unauthorized persons and misuse intelligence information for partisan political purposes. However, as discussed below, a range of measures can be applied to minimize the risk of unauthorized disclosure of information.

2.2 SECRECY AS THE EXCEPTION, NOT THE NORM

Since the abovementioned motivations for intelligence secrecy are reasonable, many articles on democratic governance of intelligence assert that "an appropriate balance must be struck between secrecy and transparency." This formulation is too non-committal to be of much value, however, and it does not have the correct point of departure. The starting point should be the fundamental tenets of democracy. These tenets include transparency and the right of persons to gain access to information held by the state. They are essential because they are prerequisites for executive accountability to parliament and other oversight bodies; effective oversight by these bodies; political and personal freedom; democratic contestation of power; robust debate and exchange of ideas; the full exercise of citizenship; and prevention of abuse of power.

The idea that freedom of information is a necessary basis for other rights and freedoms is captured in United Nations General Assembly Resolution 59(1) of 1946, which proclaims that "freedom of information is a fundamental human right and is the touchstone of all the freedoms to which the United Nations is consecrated." The same logic is evident in South Africa's Promotion of Access to Information Act of 2002, which seeks to "actively promote a society in which the people of South Africa have effective access to information to enable them to more fully exercise and protect all of their rights."

Since openness is a necessary condition of democratic governance and protection of human rights, the challenge in the world of intelligence should not be defined as "finding the right balance between secrecy and transparency." Rather, secrecy should be regarded as an *exception that in every case demands a convincing justification*. Whereas the emphasis of intelligence communities throughout the world is on secrecy with some exceptions, in democratic societies the emphasis ought to be on openness with some exceptions. This is a matter of both principle and pragmatic imperative. There is ample historical evidence that power is more likely to be abused, and human rights are more likely to be violated, in conditions of secrecy than in an open political environment. Openness permits effective oversight by parliament and scrutiny by the media and vigilant civil society groups, providing a basis for detecting illegality and misconduct and thereby for preventing the emergence of a culture of impunity.

2.3 THE RISK OF SPECIFIED HARM

What, then, is the proper basis for intelligence secrecy as an exception to openness? The common answer in democratic and authoritarian countries alike is "national security." This is an unsound and dangerous approach because of the elasticity and ambiguity of the concept of "national security."[2] If national security is interpreted broadly to cover all aspects of human security, then secrecy based on these expansive grounds can lead to excessive and spurious classification of information. Even where "national security" is defined more narrowly, it is often invoked by the state to justify extraordinary measures that violate human rights. For example, senior officials in the US Administration under President George W. Bush endorsed the use of torture in order to protect national security.[3]

In a 1971 judgement the United States Supreme Court raised concerns of this nature about the vagueness of the term "national security" in relation to restrictions on freedom of speech:

> *The word 'security' is a broad, vague generality whose contours should not be invoked*

> *to abrogate the fundamental law embodied in the First Amendment [dealing with freedom of speech]. The guarding of military and diplomatic secrets at the expense of informed representative government provides no real security for our Republic.*[4]

In a democracy the term "national security" should cover the security of the country, its system of government, its values, and all persons under the jurisdiction of the state. It consequently provides a compelling basis for openness rather than secrecy. It is not something that has to be balanced against human rights and freedoms. A democratic approach to national security encompasses and embraces human rights and freedoms.

Instead of being based on the amorphous notion of "national security," secrecy regarding the intelligence community should be motivated with reference to *specific and significant harm* that might arise from the public disclosure of information. It should be confined to those areas where public disclosure would cause significant harm to the lives of individuals, the intelligence services, the state, or the country as a whole. These areas include the following:

- the identity of intelligence officers (other than the heads of the intelligence services)
- the identity of intelligence informants
- the technical details of operational methods
- the details of VIP protection
- current operations and investigations
- the identity and personal data of individuals who are under surveillance

Depending on the circumstances, the harm arising from disclosure of information in the areas listed above might have to be weighed against a strong public interest in disclosure. Disclosure in the public interest might be appropriate if, for example, intelligence operations have illegally targeted politicians; the protection afforded to VIPs is extremely lax; or senior intelligence officers have displayed highly compromising personal behaviour. In general, democratic governments cannot seek to avoid all possible harm that might occur from the publication of sensitive information. Some harm has to be tolerated because the dangers posed by secrecy can imperil the democratic order itself.

Public and open parliamentary access to information about the intelligence community is necessarily more limited than the access enjoyed by specialized intelligence oversight bodies such as a parliamentary oversight committee and an independent inspector general of intelligence. In order to fulfil their mandates, these bodies require more information than is available in the public domain. The information needs of these bodies are discussed below.

2.4 THE PRACTICAL BENEFITS OF INTELLIGENCE OPENNESS

The preceding discussion focused on the need for intelligence openness in terms of democratic governance, respect for human rights, and prevention of abuse of power. In addition, less secrecy and greater provision of information about the intelligence services would be of benefit to the services themselves. A classification system that over-classifies information lacks credibility, is difficult to maintain and enforce, and is costly and inefficient. Too much time and effort are devoted to classifying and protecting innocuous information, potentially at the expense of safeguarding genuinely sensitive information.

In the famous 1971 US Supreme Court ruling in the *Pentagon Papers* case, Justice Potter Stewart said the following in this regard:

> *When everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion.*[5]

As noted in the introduction, moreover, greater transparency regarding the intelligence services would help to reduce public suspicion of these organizations and heighten public confidence in them. This is vital in a democracy since intelligence agencies must obtain information from individuals and communities through co-operative relationships rather than through terror and coercion.

3. LEGISLATION ON PROTECTION OF AND ACCESS TO INFORMATION

In democratic countries, the debate on intelligence secrecy and transparency outlined above is never resolved definitively and permanently. It can be a site of struggle, particularly during times of intelligence crisis and scandal, and the pendulum might swing towards greater openness or greater secrecy depending on the political and security circumstances of the country, the conduct of the intelligence services, and the perspectives of the executive, parliament, and the public.

Nevertheless, in a formal sense the debate is resolved through legislation that deals with access to and protection of state-held information. The legislation typically covers the following topics:

- the principles and criteria for classifying and disclosing information
- the authority and procedures for classification and declassification
- judicial or other high level review of classifications
- the right of individuals and public interest groups to gain access to state-held information
- the procedures for applying for such access and the right of appeal if access is denied
- the role of the courts in adjudicating disputes around classification and access
- penalties for unlawful disclosure of information

The intelligence services are usually responsible for classifying state-held information and for designing and maintaining the system of protecting classified information. They might also be involved in drafting the legislation. This creates the danger that the law will be skewed in favour of excessive secrecy. Since the intelligence services have a functional bias towards secrecy and against openness, the responsibility for drafting the legislation should lie with the ministry of justice or constitutional affairs.

Parliament and its oversight committees, such as those dealing with constitutional affairs and with intelligence, have a crucial role to play in ensuring that the legislation is consistent with democratic norms. They can improve the quality and democratic character of the law by calling on the executive to present a public motivation for the legislation and any controversial provisions; by facilitating robust debate among political parties; by holding public hearings that enable individuals, the media, and other interest groups

to comment on the draft legislation; and by amending the bill. In the final instance, the approval of the legislation lies with parliament.

In new democracies, parliamentarians might benefit from a comparative international review in order to ascertain best practice.[6] The following can be said to constitute good practice in relation to laws governing access to and protection of information:

- The legislation should acknowledge explicitly the importance of transparency and access to information as fundamental principles of democracy that promote human rights and freedoms, good governance, public accountability, and informed debate. The legislation should state that classification of information is consequently an exceptional measure that ought to be used sparingly.
- The legislation should seek explicitly to prevent inappropriate restrictions on access to information (Box 1).
- The criteria for classifying information should indicate that significant harm might arise with a reasonable degree of certainty in the event of public disclosure. The legislation should not permit resort to secrecy on the nebulous grounds of "national security" or "national interest."
- The criteria regarding disclosure and non-disclosure of information should be precise and simple in order to facilitate sound and consistent decision making by government officials and to ensure that individuals understand how they can exercise their right to obtain state-held information.
- The legislation should provide for reviews of the status of classified information at specified intervals (e.g., every five years) and the responsible officials should inform the public of the results of these reviews.
- Where a person's request for state-held information is denied, the responsible official must inform the applicant of the reason for the non-disclosure and the duration of the classification. The law should provide that the applicant may, in furtherance of a legitimate personal or public interest, request the relevant official to declassify the information. Where the official turns down the request, the applicant should be entitled to appeal against the decision. The appeal should be heard by a judge.
- The legislation should provide for the classification of *information* rather than the classification of *documents*. This would enable government officials to classify sensitive information in a document without having to classify the entire document. Such documents can then be disclosed publicly in a redacted form.
- Where classified information is relevant to court proceedings, the decision on whether to view the information in camera or in open court should be made by the judge rather than the executive.
- The legislation should enable a person charged with unlawful disclosure of classified information to raise the defence of disclosure "in the public interest." This might arise where, for example, a newspaper reveals details of illegal bugging by an intelligence services. The validity of the public interest defence should be determined by the judge who hears the case.
- The legislation should create an obligation on the executive to take steps to promote and facilitate public access to state-held information including, as discussed below, information on the intelligence services.

This list of good practice elements of legislation have as much to do with procedural as with substantive matters and relate to state-held information that includes but is not limited to information regarding the intelligence community. The following sections focus on substantive aspects of intelligence that ought to be made available to the various oversight bodies.

Box 1: Avoiding inappropriate classification of information

The US Executive Order on classification states that information cannot be classified in order to conceal violations of law, inefficiency, or administrative error; prevent embarrassment to a person, organization, or agency; or prevent or delay the release of information that does not require protection in the interest of national security. Similarly, the Slovenian Protection of Classified Information Act prohibits the classification of information relating to crimes. In Mexico and Peru, the relevant legislation prevents classification of information relating to violations of human rights and international law.[7]

4. THE INFORMATION NEEDS OF PARLIAMENT

In a democracy, the institution that bears primary responsibility for overseeing the activities of the executive and state departments is parliament. In order to fulfil this responsibility with respect to the intelligence community, parliament requires information about the following: intelligence priorities; executive policies, regulations, and actions on intelligence; intelligence assessments, budgets, and financial reports; SAI's reports on the intelligence services; the activities and findings of expert intelligence oversight bodies; and any investigations into the conduct of the intelligence services. This section considers these information needs of parliament meeting in open plenary session, as opposed to parliamentary intelligence oversight committees, which are discussed later.

4.1 NATIONAL INTELLIGENCE PRIORITIES

From time to time, typically on an annual basis, the executive has to decide what its intelligence priorities will be for the forthcoming period. This is because the intelligence services should not be self-tasking and because the prioritization of threats and areas of intelligence focus is a high level policy matter. Executive determination of intelligence priorities provides political direction to the services and serves as a basis for planning, budgeting, allocation of resources, operations, and accountability.

The executive's national intelligence priorities (NIP) should not be classified. Parliamentary discussion on the NIP would deepen accountability and democratic decision making on an aspect of national policy that affects profoundly the safety and well-being of persons under a state's jurisdiction. National security would not be undermined through disclosure since the NIP could be provided to parliament without naming specific individuals and organizations, referring instead to categories such as "organized crime," "terrorism," and "nuclear proliferation."

Sensitive information could be withheld from the version of the NIP that is presented to parliament and could be provided on a confidential basis to the parliamentary intelligence oversight committee.

4.2 EXECUTIVE POLICIES, REGULATIONS, AND ACTIONS

Executive policies and regulations on intelligence are often secret, even in well-established democracies. This is anomalous and undesirable because it violates the cardinal principle of accountability. The primary rules governing the intelligence services, especially in relation to investigative methods that infringe constitutional rights, ought to be subject to parliamentary debate and review. A distinction should be drawn between departmental rules and procedures that must be kept secret because they reveal sensitive technical details of operational methods, and executive regulations and policies that should be in the public domain because they are integral to democratic governance.

On the basis of intelligence legislation, the executive should present its policies and regulations on the following topics to parliament for consideration and comment:

- the exercise of the functions and powers of the intelligence organizations, including their powers to infringe constitutional rights
- operational policies, excluding sensitive technical details
- ministerial control and the relationship between the intelligence services and the head of state, the cabinet, and the minister responsible for intelligence
- the relationship and division of responsibilities between the various intelligence bodies, the co-ordination of intelligence, and the functions of any national intelligence co-ordinating mechanism
- relations with foreign intelligence services and the criteria and rules for sharing intelligence about individuals with foreign governments
- the disciplinary system of the intelligence services and the internal mechanisms for ensuring respect for the constitution and the rule of law

Parliament is responsible for overseeing the executive as well as state institutions. It therefore requires information about significant executive actions regarding the intelligence services. Relevant actions include the appointment and dismissal of senior staff; disciplinary action against senior staff; ministerial authorizations of intrusive operations where this is a legal requirement (see Hutton—Tool 5); and major reforms and innovations regarding the systems and operations of the intelligence community. Information that is too sensitive for the public domain should be presented to the parliamentary oversight committee on intelligence.

4.3 ANNUAL REPORTS OF INTELLIGENCE SERVICES

In a democracy, the publication of annual reports by government departments and other organs of state is a necessary means of ensuring accountability to parliament and the public at large. It provides a basis for parliament to determine whether there is adherence to government priorities and policies and whether taxpayers are getting value for money. There is no good reason to exclude the intelligence services from this practice. The annual reports of the Dutch General Intelligence and Security Service (AIVD) offer an excellent example of the provision of comprehensive and useful information without compromising national security.[8]

The annual reports of the intelligence service should cover the following matters (without divulging sensitive details): the annual objectives and priorities of the service; its assessment of major threats to security; any major reforms of intelligence policies,

systems, and operations; fulfilment of the reporting and accountability functions of the service; and the response of the service to requests for information under freedom of information legislation.

4.4 INTELLIGENCE ASSESSMENTS

In many instances the intelligence community's assessments of individuals and organizations are unsuitable for presentation to parliament because of the risk of compromising intelligence operations and criminal investigations. Yet intelligence assessments that deal with categories of security and threats to security can frequently be published without risk of harm.

By way of example, the Canadian Security Intelligence Service (CSIS) publishes a range of material, including: background papers on topics like economic security, weapons proliferation, and counter-terrorism; a publication called *Commentary* that focuses on issues related to the security of Canada; and a series of research reports based on CSIS reviews of open source information.[9] The annual reports of the Dutch General Intelligence and Security Service go so far as to include commentaries on radical and terrorist organizations that are mentioned by name.[10]

The presentation of such assessments to parliament and its intelligence oversight committee(s) is an important form of accountability, enabling parliamentarians, academics, and non-governmental organizations to debate the political and security perspectives of the intelligence services. Over time, informed parliamentary and public discussion might lead to refinements in these perspectives.

4.5 BUDGETS, FINANCIAL REPORTS, AND REPORTS OF SUPREME AUDIT INSTITUTIONS

In democratic countries parliament receives, reviews, and debates the annual budgets and financial reports of government bodies. This is an indispensable form of accountability, enabling the elected representatives of the people to oversee and approve the use of public funds in accordance with legislation, government policy, and parliament's own priorities and preferences. The full versions of the financial reports and budgets of the intelligence services, however, are typically presented only on a confidential basis to a parliamentary oversight committee and are not tabled in parliament as a whole (see Wills—Tool 8).

Intelligence organizations are resistant to revealing their budgets on the grounds that foreign intelligence services would thereby gain an advantage over them. This argument is overstated. A foreign service would derive no benefit from knowing how much money another country spends on its intelligence services. Nor indeed would any advantage or prejudice arise from disclosing the spending breakdown on personnel, operating costs, and capital expenditure. It is only at a much higher level of detail—regarding targets, methods, sources, and operational outputs and constraints—that security could be undermined through disclosure (see Box 2).

Box 2: Publication of intelligence budgets and financial reports

In 2006, the Ministerial Review Commission on Intelligence in South Africa scrutinized the classified budgets, financial reports, and strategic plans submitted annually by the intelligence services to the parliamentary intelligence oversight committee. The Commission concluded that the publication of these documents would not in any way compromise intelligence operations or the security of the country. The Commission agreed with the National Treasury's view that the intelligence budgets and financial reports should be presented openly to parliament. Sensitive details could be limited to the documents that are considered in closed sessions of the oversight committee.[11]

Similarly, a SAI's annual report on the intelligence services should have two versions: a public report that is presented to parliament and a classified report with greater detail that is presented to the relevant parliamentary oversight committee. The legislation governing the reports of the auditor-general should provide for the protection of sensitive information (see Box 3).

Box 3: Protecting sensitive information in financial audits

South Africa's Public Audit Act of 2004 contains several provisions on protection of sensitive information. It states that the auditor-general must take precautionary steps to guard against the disclosure of secret or classified information obtained in the course of an audit. When reporting on a confidential security account, the auditor-general "must have due regard for the special nature of the account and, on the written advice from the relevant Minister, on the basis of national interest, may exclude confidential, secret or classified details of findings from the audit report, provided that the audit report states that these details were excluded."

4.6 DEALING WITH INTELLIGENCE SCANDALS

The preceding discussion focused on the intelligence information that parliament requires as a matter of course in order to fulfil its oversight responsibility. If there is a crisis involving the intelligence services (e.g., revelations of spying on politicians), parliament can establish a commission of inquiry or request one of the specialized intelligence oversight bodies to conduct an investigation. The findings of the investigation should be presented to and debated openly by parliament. If this is not done openly, there will be no public confidence in the investigation and no public assurance that any wrongdoing has been dealt with properly.

5. THE INFORMATION NEEDS OF SPECIALIZED INTELLIGENCE OVERSIGHT BODIES

The information needs of specialized intelligence oversight bodies—foremost of which are a parliamentary intelligence oversight committee, an independent inspector general of intelligence, and an expert intelligence oversight body (such as the Review Committee on the Intelligence and Security Services in the Netherlands)—derive from the mandate and functions of these bodies. The mandate and functions differ from one country to another but may include the following:

- compliance by the intelligence services with the constitution, legislation, regulations, and government policies
- the performance and success of the intelligence services in terms of their legislative mandate and functions and the priorities set by government
- internal systems and methods for preventing, detecting, and addressing misconduct
- internal financial systems and spending

In view of these oversight functions, this section considers the information needs of a parliamentary intelligence oversight committee; an independent inspector general of intelligence and other ombuds institutions; and the judiciary. The section then looks at ways of minimizing the risk of inadvertent or deliberate disclosure of classified information.

5.1 PARLIAMENTARY INTELLIGENCE OVERSIGHT COMMITTEES

The parliamentary intelligence oversight committee would naturally receive all the information on intelligence that is presented to parliament as whole. The committee would usually receive this information first so that it has an opportunity, prior to the parliamentary debate, for careful scrutiny, deliberation, and interaction with senior intelligence officers and the member(s) of the executive responsible for intelligence. The committee as a collective and its members who represent different political parties are then equipped to make well-informed inputs to the broader parliamentary debate.

In addition, the oversight committee should receive, on a confidential basis, more detailed and more sensitive information than that which is presented to parliament as a whole. The topics on which it should receive detailed information include the following:

- the executive's national intelligence priorities
- executive policies, regulations, and actions on intelligence
- the annual reports of the intelligence services
- the security and threat assessments of the services
- the annual budgets and financial reports of the services
- the SAI's reports on the services
- the activities and findings of expert intelligence oversight bodies (if they exist)

The crucial and difficult question is how much detail and what level of sensitivity should be presented to the oversight committee. On the one hand, the members of the committee are not trained in the maintenance of secrecy, and they are bound to have mixed political loyalties to both their country and their political party. Moreover, it is axiomatic that the greater the number of people who are in possession of secret information, the less likely it is that the information will remain secret. The intelligence services are therefore reluctant to disclose sensitive details about their operations, methods, and personnel. On the other hand, the parliamentary committee must receive sufficiently detailed information to perform its oversight functions adequately. If too much information is withheld, the oversight will be superficial and will not detect or examine properly any misconduct, poor performance, or misuse of funds.

The question of how much detail and what level of sensitivity should be presented to the parliamentary oversight committee must be addressed in legislation, as precisely as

possible, in order to minimize the potential for misunderstanding and disputes between parliament and the intelligence services and/or the executive branch. The way in which such rules and guidelines are formulated in legislation differs from one country to another (see Box 4 for several examples).

Box 4: Legislative provisions on access to information by parliamentary oversight committees

In Romania the intelligence services are obliged to meet the information requests of the parliamentary intelligence oversight committee within a reasonable period unless doing so would jeopardize on-going operations, the identities of agents, methods, or sources. The parliamentary committees may conduct unannounced visits to the services and must be given full access to personnel, data, and facilities.[13] In the United Kingdom, by contrast, the parliamentary oversight committee's current mandate is limited to "the expenditure, administration and policy" of the intelligence and security services, implicitly excluding operations from the committee's ambit and thus limiting its access to information.[14]

Legislation should also specify the means of resolving disputes on access to information by the parliamentary committee. In South Africa, for example, the relevant law states that disputes will be resolved by an ad hoc committee comprising the minister for intelligence, the head of the intelligence service, the chairperson of the parliamentary oversight committee, and the inspector general of intelligence.[12]

The parliamentary oversight committee's powers to obtain information regarding intelligence differ from one country to another. As a matter of routine, the committee should receive regular reports from the following: the member(s) of the executive responsible for intelligence; the intelligence services; the SAI; the judge or executive member responsible for authorizing intrusive operations; and any expert intelligence oversight bodies that exist. The committee should also be empowered to request a report from any of these entities. In addition, it can have the power to conduct an inquiry, to subpoena witnesses, and to inspect intelligence premises.

5.2 INSPECTORS GENERAL OF INTELLIGENCE AND OTHER OMBUDS INSTITUTIONS

The secrecy that surrounds intelligence services poses substantial difficulties for effective oversight. There is consequently a need for intelligence oversight bodies that have special powers and specialist expertise. One such body is an independent inspector general of intelligence (IG).[15] In order to perform effective oversight in a secret environment, the IG must have the following attributes:

- The IG must be an independent official with security of tenure.
- He/she must have the legal mandate and powers to monitor the services' compliance with the constitution, legislation, and government policies, as well as to investigate complaints of misconduct, illegality, and abuse of power.
- The IG must report not only to the minister responsible for intelligence but also to the parliamentary intelligence oversight committee and, in the case of major investigations, to parliament as a whole.
- The IG and his/her staff must have a high level of expertise and experience in intelligence.

In addition, the legislation governing the IG must provide that the inspector general and his/her staff may not be denied access to any intelligence, information, or premises under the control of the intelligence services, and that any denial of such access constitutes a criminal offence. These are essential requirements when an independent oversight body investigates secret operations and systems.

The preceding comments about the IG apply equally to other ombuds institutions, such as human rights commissioners, in countries where there is no inspector general for intelligence. The big advantage of the specialist IG approach is that the inspector general and his/her staff have expertise in intelligence, equipping them both to detect malfeasance in a secret environment and to protect properly the classified information to which they have access.

When auditing the spending, budgetary allocations, income (if any), and financial systems of the intelligence services, the SAI should have access to all information concerning the secret operations and secret funds of the services (see Wills—Tool 8 for further information). Accordingly, the SAI should have a specialist team that has been trained to deal with classified documents and has received security clearance. Alternatively, it might be appropriate for the office of the independent inspector general of intelligence to conduct the financial audit in co-operation with the SAI.

5.3 JUDICIARY

The intelligence services and law enforcement agencies infringe the right to privacy when they conduct intrusive operations such as interception of communication and search and seizure. Consequently, in most democratic countries government bodies must obtain judicial authorization to undertake these operations (see Hutton—Tool 5 for further discussion). Depending on the country, the agencies might be able to approach any judge for this purpose or there might be a dedicated judge who considers all the interception applications.

The information required by the judge is usually spelt out in legislation on interception of communication. The applicant has to provide sufficient facts to satisfy the judge that the interception is a necessary and justifiable means of gathering information about criminal activity or a threat to national security or public safety. The legislation might regard the interception of communication as a method of last resort, in which case the applicant must also convince the judge that non-intrusive methods are inadequate or inappropriate.

Aside from the issue of interception applications, criminal or civil cases involving the intelligence community might come before the courts if, for example, an intelligence officer is charged with an offence or a politician alleges that his/her office has been bugged illegally. The executive might want to have some or all of such cases heard in camera. Democracies differ on how this problem is addressed. The matter might be covered by legislation or it might be left to the discretion of the presiding judge (Box 5).

Box 5: Dealing with sensitive information in court proceedings

In a case considered by the Constitutional Court in South Africa in 2008, a newspaper group sought an order to compel public disclosure of restricted portions of the record of judicial proceedings involving the National Intelligence Agency (NIA). It based its application on the right to open justice. The Minister of Intelligence objected to the disclosure on the grounds of national security. The Court ordered the release of some of the material, finding that there was no valid national security basis for non-disclosure, but held that other information—regarding relations with foreign intelligence services, the chain of command within NIA, and the identity of NIA operatives—must remain restricted. A minority opinion held that it was in the public interest to release all the material except for the names of certain operatives.[16]

5.4 ENHANCING THE ACCOUNTABILITY OF OVERSIGHT BODIES

Democratic countries can have relatively strong parliamentary and independent oversight of the intelligence services and yet the oversight bodies may not be adequately accountable to the public. The oversight bodies are themselves too secretive. This undermines public confidence in both the oversight bodies and the intelligence services. It is thus incumbent on the oversight bodies to present meaningful reports to parliament and to publish their reports, as well as reports from the intelligence services, on their web sites. A good example of this practice is the Review Committee on the Intelligence and Security Services in the Netherlands, which publishes annually a comprehensive report on its monitoring and investigations.[17]

5.5 MINIMIZING THE RISK OF DISCLOSURE OF CLASSIFIED INFORMATION

As noted previously, the intelligence services are sometimes resistant to disclosing sensitive information to parliamentary oversight committees because the members of these committees are politicians and are usually untrained in the discipline and practices of safeguarding classified information. There is consequently a risk of deliberate or inadvertent disclosure of sensitive information. The following steps can be taken to minimize this risk:

- Legislation on protection of information makes the unauthorized disclosure of classified information a criminal offence.
- The members of parliamentary oversight committees are subject to vetting by an intelligence service prior to their appointment to the committee.[18]
- The committees are empowered by law to hold meetings in camera.
- Intelligence experts ensure that the oversight committees' offices, computers, telephones, and filing systems are protected against surveillance.
- Intelligence experts provide education and training to members and staff of the committees.
- The committees and the intelligence services jointly agree on rules and procedures regarding the receipt, possession, use, and destruction of classified information.

The above measures are also relevant in whole or in part to other specialist oversight bodies. However, where these bodies comprise professionals as opposed to politicians, the risk of disclosure of classified information might be lower.

6. RECOMMENDATIONS

- Transparency and access to state-held information are necessary conditions for democratic governance, protection of human rights, and prevention of abuse of power. Secrecy should thus be exceptional. With respect to the intelligence community, secrecy should be based on specific and significant harm that might arise from the disclosure of information. It should be confined to those areas where disclosure would cause serious harm to the lives of individuals, the intelligence services, the state, or the country as a whole. The harm arising from disclosure might have to be balanced against a compelling public interest in disclosure.
- The responsibility for drafting legislation on protection of and access to information should lie with the department of justice or constitutional affairs and not with the intelligence services. Parliament should endeavour to ensure that the legislation is consistent with democratic norms.
- The legislation should emphasize that transparency and access to information are fundamental principles of democracy and that classification of information must be used sparingly. The criteria for classification should indicate a sufficient degree of harm and certainty to warrant non-disclosure. The legislation should enable a person charged with unlawful disclosure of classified information to raise a public interest defence. The executive should be obliged to promote and facilitate public access to state-held information, including information on the intelligence services.
- Parliament requires information about the following: intelligence priorities; executive policies, regulations, and actions on intelligence; intelligence assessments, budgets, and financial reports; SAI reports on the intelligence services; the activities and findings of expert intelligence oversight bodies; and any investigations into the conduct of the intelligence services. The parliamentary intelligence oversight committee should receive on a confidential basis more detailed and more sensitive information on these topics. The information must be sufficient for the committee to perform its oversight functions adequately. The details in this regard should be specified in legislation.
- The legislation governing the inspector general of intelligence and/or the expert intelligence oversight body must provide that the entity and its staff may not be denied access to any intelligence, information, or premises under the control of the intelligence services, and that any denial of such access constitutes a criminal offence.
- In criminal or civil cases involving the intelligence services, the decision on whether to hear some or all of the case in camera should be made by the presiding judge.
- The oversight bodies should present meaningful reports to parliament and should publish their reports, as well as reports from the intelligence services, on their web sites.
- Steps can be taken to reduce the risk that members of the parliamentary intelligence oversight committee deliberately or inadvertently disclose classified information: the members can be vetted by an intelligence service; they can be trained to protect classified information; and their offices, computers, telephones, and filing systems can be protected against surveillance.

Endnotes

1. This tool draws on my experience and research as a member of the Ministerial Review Commission on Intelligence, established by the South African Minister of Intelligence in 2006. The tool also draws on L. Nathan, *Lighting up the Intelligence Community: A Democratic Approach to Intelligence Secrecy and Openness*, Policy Paper (Birmingham, UK: Global Facilitation Network for Security Sector Reform, 2009).
2. For a detailed discussion of this point, see A. Wolfers, "'National Security' as an Ambiguous Symbol," *Political Science Quarterly* Vol. 67, No. 4 (1952), pp. 481–502.
3. American Civil Liberties Union, *The Torture Report* web site (available at www.thetorturereport.org).
4. *New York Times Co vs United States* 403 US 713 (1971) at 719.
5. *New York Times Co vs United States* 403 US 713 (1971).
6. For an example of such a review, see D. Banisar, "Public Oversight and National Security: Comparative Approaches to Freedom of Information," in *Democratic Control of Intelligence Services: Containing Rogue Elephants*, eds. H. Born and M. Caparini (Aldershot, UK: Ashgate, 2007), pp. 217–235.
7. The information in this box is drawn from Banisar, "Public Oversight."
8. These reports can be found on the web site of the Dutch General Intelligence and Security Service (available at https://www.aivd.nl/english/). For the 2010 report, see https://www.aivd.nl/english/publications-press/@2827/annual-report-2010/.
9. See the web site of the Canadian Security Intelligence Service (available at www.csis-scrs.gc.ca).
10. See Banisar, "Public Oversight."
11. South Africa, Ministerial Review Commission on Intelligence, *Intelligence in a Constitutional Democracy: Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP* (10 September 2008) (available at www.ssronline.org/document_result.cfm?id=3852).
12. South Africa, Intelligence Services Oversight Act, Act No. 40 of 1994, Section 4(2)(b).
13. C. Matei, "Romania's Transition to Democracy and the Role of the Press in Intelligence Reform," in *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness*, eds. T. Bruneau and S. Boraz (Austin: University of Texas Press, 2007), p. 227.
14. P. Gill, "Evaluating Intelligence Oversight Committees: The UK Intelligence and Security Committee and the 'War on Terror,'" *Intelligence and National Security* Vol. 22, No. 1 (February 2007), pp. 14–37.
15. A distinction should be drawn between an inspector general of intelligence that is an independent statutory office (as in Australia, New Zealand, and South Africa) and one that is located within an intelligence organization (as in the Central Intelligence Agency of the United States).
16. *Independent Newspapers (Pty) Ltd vs Minister for Intelligence Services* CCT 38/07 [2008] ZACC 6 (South Africa).
17. The annual reports of this committee can be viewed at http://www.ctivd.nl/.
18. For more information on the vetting of members of parliamentary oversight committees, see H. Born and I. Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Geneva: DCAF, University of Durham, and Parliament of Norway, 2005), pp. 88–90.

TOOL 4

Conducting Oversight

Monica den Boer

FOUR

4

Conducting Oversight

Monica den Boer

1. INTRODUCTION

In new democracies, effective oversight of the intelligence community is crucial because of the inherent tension that exists between intelligence work and certain democratic values, such as openness and transparency. If national intelligence services are to be brought under external civilian control, civilians must become educated about intelligence work. Otherwise, the work will continue to be monopolized by service professionals. A new political culture must also be developed that prevents abuse while still supporting the legitimate role of intelligence services in a democratic society.

This tool explains how oversight bodies investigate the activities of intelligence services. It considers the widest possible range of oversight, from ad hoc investigations to long-term inquiries. In addition, it considers those situations in which multiple standing bodies have oversight responsibilities and those in which no permanent body exists, requiring the creation of a temporary body.

Moreover, this tool is intended to serve as a practical guide to how intelligence oversight is conducted. Because oversight bodies in different countries are confronted with many similar challenges, understanding basic methodology can help new oversight bodies avoid common pitfalls and maximize their effectiveness.

2. REASONS FOR CONDUCTING INTELLIGENCE OVERSIGHT

Intelligence accountability has many layers. Some of these relate to the control of intelligence services as practiced internally by service officials and externally by members of the executive. Others relate to oversight as practiced by parliament, the judiciary, and expert oversight bodies (see Born and Geisler Mesevage–Tool 1). The fundamental purpose of intelligence oversight is to discourage improper activity on the part of national intelligence services. As opposed to *control*, which refers to the direct management of a service, *oversight* includes monitoring, evaluation, scrutiny, and review. By promoting openness and transparency, oversight bodies can restrain abusive tendencies within a service and provide members of parliament and the executive (and others who exercise control responsibilities) with useful information and expertise.

2.1 HUMAN RIGHTS VIOLATIONS

The possible violation of human rights by intelligence services is always a reason for public concern. During the 1960s and 1970s, for instance, US government agencies authorized aggressive covert intelligence operations against the civil rights and antiwar movements. More recently, national intelligence services cooperating on counter terrorism have utilized such practices as extraordinary rendition, the operation of secret detention centres, and the use of information obtained by torture. These practices, which manifestly threaten human rights, are all appropriate matters for oversight.

Inappropriate and/or illegal activities are often brought to the attention of oversight bodies by the media, especially by investigative journalists acting on tips from non-governmental organizations such as Human Rights Watch and Amnesty International. According to Marina Caparini,

> *"The media constitute an interconnective tissue linking individuals and groups with government and play a critical role in conveying information about shifts in public opinion and policy preference…It is primarily through a free press that publics can be informed and government held to account via the threat of public scrutiny of its decisions, actions, and abuses of power."*[1]

2.2 PARLIAMENTARY QUESTIONS

Members of national parliaments, even those who do not belong to oversight committees, can raise questions about the activities of intelligence services. These can range from general questions about threat levels and service priorities to specific questions about covert methods and interactions with particular groups. Sometimes the questions can identify legal voids that emerge when a new operation is initiated for which no oversight mechanism yet exists. In 2003, for instance, Dutch parliamentarians raised questions about intelligence gathering with regard to weapons of mass destruction allegedly held by the former government of Saddam Hussein in Iraq.[2] These questions led to the establishment of the Dutch Committee of Inquiry on Iraq.

3. OVERSIGHT MANDATES

Intelligence services must comply with the laws, directives, warrants, and policies of the

governments that they serve.[3] Intelligence oversight bodies must similarly respect the laws, or mandates, that both establish and limit their investigative powers. Oversight mandates are usually drafted in the most neutral manner possible so as to avoid political controversy. This is particularly important when the oversight body is temporary, as in the case of an ad hoc inquiry into a specific incident. Nevertheless, mandates need to be specific and clear and commensurate with the powers, methods, and resources of the service(s) being overseen.

The mandates of oversight bodies may be complementary, or they may overlap. The latter is preferable because a single oversight mechanism is generally considered insufficient. For this reason, the intelligence oversight system in Italy was recently expanded from merely *ex post* oversight by the Constitutional Court to include two new mechanisms: an internal administrative body (the Office of the Inspector General) and an external political body (the Parliamentary Committee for the Security of the Republic [COPASIR]).[4] The Canadian Security Intelligence Service (CSIS) has four overlapping oversight mechanisms: an Inspector General, who monitors CSIS compliance with operational policies; a Security Intelligence Review Committee (SIRC), which reviews CSIS activities and investigates complaints against the service (see Farson–Tool 2); the Federal Court of Canada, which is the only body authorized to permit the use of special investigative measures;[5] and public reporting, in the form of the Minister for Public Safety's Annual Statement on National Security and the CSIS Public Report.[6]

The mandate of a parliamentary oversight committee such as COPASIR should cover a nation's entire intelligence community, including supporting departments and officials.[7] The mandate should give the committee all the authority it needs to monitor the legality, efficacy, and efficiency of the intelligence services, as well as their budgeting and accounting practices, compliance with human rights standards, and other policy/administrative aspects. When a mandate fails to do so, it should be revised. For instance, when an Australian ad hoc inquiry found that the Defence Imagery and Geospatial Organization (DIGO) was not sufficiently accountable because of a restricted oversight mandate, the inquiry recommended that the mandate of the relevant parliamentary oversight committee be extended to include all of Australia's intelligence services. The inquiry also recommended that the mandate of the Inspector General of Intelligence and Security be widened to include monitoring of DIGO (see Born and Geisler Mesevage–Tool 1).[8]

3.1 TYPES OF MANDATES

Mandates can be broad or narrow. For instance, the mandate of one oversight body may be simply to verify the legality of the activities of a single intelligence service. Another body may be charged with reviewing the effectiveness of multiple agencies, including the performance of officials and the conduct of the budgetary process. Wider mandates generally help to avoid fragmented or otherwise imperfect oversight.

Oversight mandates sometimes include powers that extend beyond those strictly necessary for the performance of monitoring. For instance, they can include the powers of arrest and pretrial detention, as well as the use of lethal force. They can also include control of the transfer of information to foreign services and approval of executive appointments to top intelligence positions.[9]

With regard to covert activities, especially those that utilize special investigative measures to collect personal data, oversight mandates sometimes include preventive or proactive powers. For example, in Belgium, the Special Intelligence Act authorizes the Standing Intelligence Agencies Review Committee (Committee I—an expert oversight body) to advise intelligence services on the use of special investigative measures. If this advice is negative, the services may not appeal. Furthermore, should the Standing Committee identify illegal practices during its monitoring of the use of special investigative measures, it can suspend them.[10]

Oversight mandates can also include budgetary scrutiny. In the UK, for instance, intelligence service accounting is audited by the National Audit Office and also scrutinized by the parliamentary Intelligence and Security Committee, whose annual report makes public some details of intelligence service funding and expenditures.[11] Similarly, the South African Joint Committee on Intelligence scrutinizes the financial management of that country's intelligence services;[12] while in Poland, the parliamentary oversight committee reviews draft intelligence budgets and monitors their implementation. Some states go so far as to include budgetary control in the mandates of their oversight bodies. For example, the Argentinean Bicameral Committee for the Oversight of Intelligence Bodies and Activities and the US congressional intelligence committees both have this power.

3.2 CHANGES IN MANDATES

The mandates of intelligence oversight bodies need not be fixed. For instance, when the mandate of an intelligence service is expanded, the mandate of the body that oversees its activities should also be revised.[13]

Strategic events with significant political fallout can also prompt changes in the mandates of intelligence oversight bodies, especially when those events involve intelligence failures. For instance, the US intelligence community's failure to detect and prevent the 9/11 attacks led to a reconsideration of intelligence-sharing mechanisms. Changes to those mechanisms impacted the work of oversight bodies, necessitating a change in their mandates as well.

At other times, oversight bodies, through the course of their work, identify for themselves changes that need to be made in their mandates. For this reason, some oversight bodies perform regular strategic reviews to identify and recommend such changes. In these ways, oversight bodies can turn deficiencies into positive, constructive recommendations for an improved intelligence sector.

4. OVERSIGHT POWERS

The powers granted to intelligence oversight bodies vary greatly. Those described below are among the most common. The list, however, is not complete. For instance, some mandates include the power of referral, which authorizes the oversight body to refer a finding of misconduct to an internal body (such as an inspector general) for disciplinary action, or to an external body for criminal prosecution. The power of exposure is the power of oversight bodies to expose non-compliance, errors of judgement, or violations of the law to the highest authority in the relevant state, such as the Attorney General in the United States—which goes beyond reporting to an inspector general.

4.1 INFORMATION RIGHTS

Information rights, which give oversight bodies access to information, may be passive or active. An oversight body with passive information rights can receive information about intelligence activities in document form and through briefings. Ideally, such briefings are current and comprehensive; but, depending on the prevailing laws, they may not include highly sensitive information such as budgetary matters and covert operations.

Oversight bodies with only passive information rights are completely dependent on the agencies they oversee for the breadth and accuracy of the information they receive. For this reason, it is preferable for oversight bodies to have both passive and active information rights. Oversight bodies with active information rights are entitled to seek out the information that they require—for instance, by compelling officials to provide the information or by making unannounced visits to the service's premises.

Although oversight bodies should have unlimited access to all the information they require in order to discharge their duties, this is not always the case. For instance, most oversight bodies have access to classified information, but some do not. On the other hand, some restrictions may be sensible, such as those that protect the identities of sources. Such restrictions apply, for example, to access to information by South Africa's parliamentary Joint Standing Committee on Intelligence. In Argentina, Canada, and the United States, certain oversight bodies have unlimited access to information.

4.2 INVESTIGATIVE POWERS

Beyond the mere ability to scrutinize information provided to them, intelligence oversight bodies need the power to initiate investigations. The Dutch Review Committee on the Intelligence and Security Services (CTIVD), for example, has the power to initiate investigations based on complaints it receives against intelligence services. The mandates of other oversight bodies empower them to initiate investigations on their own, without the basis of a complaint. Specific investigative powers include the authority to request and/or compel officials to appear before the oversight body to answer questions.

4.3 APPROVAL POWERS

Some mandates give oversight bodies the right to approve, or authorize, strategic intelligence programmes, service budgets, and/or top-level appointments. Oversight bodies possessing one or more of these approval powers can use them to exercise meaningful influence over the services they oversee, especially in the setting of intelligence priorities. For instance, the "power of the purse" exercised by the US congressional intelligence committees is considered a strong tool for oversight and control because it allows the committees to indicate intelligence and policy priorities through monetary allocations.

5. OVERSIGHT METHODS

In addition to defining powers, an oversight body's mandate should define the methods it can use to conduct investigations. Those most frequently utilized are inspections, hearings, and documentary analysis. Other methods include interviews, witness statements, and direct access to databases (the last of which Belgian and Dutch officials consider a key method of oversight). All are used individually, in tandem, and in sequence to pursue the goals of oversight.

5.1 INSPECTIONS

Some oversight bodies perform regular inspections of the premises of the intelligence services they oversee. These visits may take place annually, quarterly, or even monthly. In most cases, oversight bodies inform intelligence services of forthcoming visits, but many also have the power to conduct an unannounced inspection. During the visits, members of the oversight body may interview employees or examine computer databases using techniques such as random sampling. In Norway, the parliamentary intelligence oversight committee (known as the EOS Committee) conducts multiple inspections each year; in the Netherlands, the CTIVD has a similar mandate. In New Zealand, the Inspector-General of Intelligence and Security has the authority to enter service premises but only if prior notice has been given to the service director.[14]

5.2 HEARINGS

Hearings are a common way for oversight bodies to obtain information from intelligence officials, independent experts, and other respondents. Although laborious and sensitive, they can be essential to the reconstruction of a narrative for which the documentary record is weak or has been obscured. Hearings can also help to assign political and/or executive responsibility for decisions made and/or implemented by intelligence and other officials. The current UK inquiry into national involvement in the Iraq war, chaired by Sir John Chilcot, has held numerous public hearings, all of which have been broadcast in real time.[15] The Dutch Committee of Inquiry on Iraq held similar hearings but not in public.

5.3 DOCUMENTARY ANALYSIS

Oversight bodies regularly review classified and unclassified reports and other documents produced by intelligence services. These documents often provide useful information and may answer some questions; but they may also raise other questions concerning the work of intelligence services that have to be answered in other ways.

Documentary analysis need not be limited to documents produced by the intelligence services. The Dutch Committee of Inquiry on Iraq, for example, created a public web site to solicit other documents that might be helpful.

6. OVERSIGHT TIMING

Oversight can take place before a decision has been made regarding an operation or policy, while it is being implemented, or after it has been implemented. The timing of the oversight depends on the mandate of the oversight body (see Born and Geisler Mesevage–Tool 1).

6.1 *EX POST* OVERSIGHT

The most common form of oversight is *ex post* oversight. The underlying rationale is that oversight bodies should review, but not interfere with, the management decisions of intelligence services.[16] *Ex post* oversight does not necessarily preclude the briefing of oversight bodies about planned or ongoing operations, but it does strongly imply that the oversight body will take a retrospective view of events, scrutinizing only those that have already occurred.

6.2 *EX ANTE* OVERSIGHT

Some intelligence oversight bodies have a mandate to perform *ex ante* oversight. *Ex ante* oversight is regarded as a way to enhance the authority of the oversight system. This implies inspection and/or approval of intelligence activities before they are initiated. One can also speak of a "proactive mandate," which is defined as "a mandate that allows the oversight body to veto or alter the policy or functioning of the services before the policy or operation is put into practice."[17] Many oversight bodies are in the position to scrutinize the policy and strategy of relevant intelligence services, and they may ask or instruct internal review bodies to conduct an investigation prior to the start of a specific intelligence activity or covert operation.

The UN special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism recommends *ex ante* oversight, which he considers to be useful for preventing human rights violations by intelligence services in the fight against terrorism. Similarly, it is recommended that oversight bodies conduct *ex ante* review of cooperation agreements between domestic intelligence services and foreign partners before those agreements are signed (see Roach–Tool 7).[18]

On the other hand, oversight bodies conducting *ex ante* review may sometimes be held responsible for intelligence failures and violations of the law that occur as the result of approved activities. The ability of an oversight body to conduct *ex ante* review may also preclude relationships with foreign partners who prefer not to disclose confidential information to oversight bodies.[19]

Many domestic intelligence services have similar security concerns regarding the advance disclosure of operational information, especially when members of parliament are involved. For this reason, members of parliament who sit on intelligence oversight committees often have to undergo security vetting. Sometimes not even this precaution is considered sufficient.

6.3 PERIODIC OVERSIGHT

Oversight can also take place on a periodic basis. Intelligence service mandates often require senior management to prepare regular (typically annual) reports on service activities for submission to the executive, parliament, or both. Likewise, oversight bodies can perform their scrutiny in a cyclical rather than episodic manner. Acknowledging that its capacity is limited, Canada's SIRC has adopted a plan that provides for the oversight of all aspects of the intelligence services on a three- to five-year cycle. The report of the ad hoc inquiry into Australia's intelligence services (discussed above) similarly recommended that reviews of the intelligence community take place every five to seven years.[20]

7. OVERSIGHT INVESTIGATIONS

Oversight investigations can be initiated in many different ways. Members of parliament or the executive can formally request them. The media can agitate for them. In some countries, such as Belgium and Canada, a complaint made by a member of the public will trigger one. Often, oversight bodies are empowered to initiate their own investigations. In most cases, however, oversight bodies reserve to themselves the final decision on whether or not to take up a particular issue.

7.1 INVESTIGATIONS OF SPECIFIC CASES

Overseers may initiate investigations into specific cases on the basis of allegations made, for instance, by complainants, parliamentarians, or the media. Overseers may conduct investigations into specific events or allegations concerning intelligence services, and these investigations may be initiated by the overseer. According to relevant procedures, intelligence services may provide the overseer with reports on serious incidents, which may concern, for instance, illegal activities, breaches of security, or the leakage of information. These reports may be provided either on a regular basis or submitted to ad hoc inquiries. Such a report was prepared by the Royal Canadian Mounted Police (RCMP) for the Canadian Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. This inquiry established inter alia that the RCMP had not complied with its own policies requiring the screening of personal data for relevance and reliability before it is shared with other intelligence services. Among the Commission's twenty-three recommendations was an admonition that the RCMP stay within its mandate as a police force.[21]

7.2 THEMATIC INVESTIGATIONS

Thematic investigations focus on broad issues rather than specific events. They sometimes arise from inquiries into specific events whose findings bring more far-reaching concerns to light.

Box 1: The Dutch parliamentary inquiry into special investigative measures: a case study in thematic oversight

In 1993, a Dutch interregional criminal investigative team assigned to collect intelligence on a drug trafficker used special investigative measures to carry out its task. Allegedly, these measures included illegal acts, notably the controlled release of drugs onto the market. In response to the allegations of misconduct, the team was disbanded, and in April 1994 the Dutch Parliament initiated a formal inquiry into the use of special investigative measures by Dutch authorities.[22]

The inquiry began with documentary analysis and orientation talks involving politicians and intelligence professionals. In addition, the inquiry commissioned academics to prepare two reports: an assessment of the nature, seriousness, and volume of organized crime in the Netherlands; and a comparative international study of legislation regulating the use of special investigative measures.

Meanwhile, the inquiry's staff (all of whom were subject to security vetting) held six months of closed hearings. The purpose of these hearings was to gather information about and insight into the use of special investigative measures in the Netherlands. The closed hearings also served as preparation for a series of open, public hearings that were broadcast directly.

The inquiry, which ended in 1996, produced an elaborate report, 6,700 pages long with 129 recommendations. Two years later, Parliament created a new, temporary committee to evaluate implementation of those recommendations. The new committee developed much new information, including evidence of drug-related corruption within the police and the customs service. These revelations nearly forced Minister of Justice Benk Korthals from office, but he managed to survive the parliamentary debate.

8. ORGANIZING OVERSIGHT

Because the most effective oversight is systematic, it is instructive to break down the oversight process into distinct, sequential phases.

8.1 IDENTIFYING AND SELECTING THE ISSUES

Intelligence work is a complex, dynamic field involving multiple actors, procedures, and policies. For this reason, a wide range of issues can become the subject of intelligence oversight. The best way to begin an oversight process is to compile an inventory of all possible issues and compare that inventory to the oversight body's legal mandate. Areas of overlap point to appropriate subjects for scrutiny.

8.2 OBTAINING SECURITY CLEARANCES

Members and employees of oversight bodies generally need to obtain security clearances in order to handle classified information. Notable exceptions are members of parliamentary oversight committees, who tend to resist investigation of their personal lives, especially when the intelligence service carrying out the background checks is paradoxically the same entity being reviewed or investigated. Nevertheless, the exclusion of politicians from security vetting is highly controversial.

8.3 SECURING THE OVERSIGHT BODY'S OFFICE

The office of the oversight body should be secure. For instance, it should be swept regularly for electronic surveillance devices. In addition, computers and other information-technology apparatus should be password protected and encrypted. Similarly, all support personnel who have access to the premises (including secretaries, translators, caterers, and cleaners) should undergo security checks.

8.4 SECURING DOCUMENTS AND OTHER MATERIALS

Members of oversight bodies should be stringent in their handling of documents and notes. A clean-desk policy should be observed, with classified information routinely stored in safes. Classified documents, whether printed on paper or stored digitally on a computer or flash drive, should never leave the office without proper authorization. Internal records relating to confidential sources, witnesses, and other key respondents should be held anonymously. Finally, all of these requirements should be stated explicitly in an internal manual of proper procedures.

8.5 MAKING A PLAN

Some oversight bodies are required to prepare sets of regulations or protocols or even detailed inspection plans and have them approved before they can begin any oversight activities. The purpose of this exercise is to avoid misunderstandings regarding the rights and powers of the oversight body and those of the intelligence service being overseen. Among the specifics minimally included in such documents are the identity of the unit or mission being scrutinized, the technologies involved, and the files that will be subject to inspection.

Box 2: Elements of a basic inspection plan

- date of the inspection
- legal basis for the inspection
- purpose of the inspection
- objectives of the inspection
- names of the oversight personnel who will perform the inspection
- designations of the service units to be inspected
- names of the service personnel to be interviewed
- interview requirements
- list of the documents to be inspected
- preinspection document request
- resources
- administrative assistance
- reporting timeline[23]

Box 3: Additional tasks for a detailed inspection plan

- Make an inspection timetable.
- Draft a list of respondents.
- Draft a letter of invitation to potential respondents and a letter of request to the supervisors of respondents whose testimony requires authorization.
- Develop a protocol for managing respondents with diplomatic status (privileges and immunity).
- Decide on the types of interviews to be conducted (confidential, anonymous, recorded, etc.).
- Develop protocols for the interviews, addressing such issues as: Will the respondent have prior access to the questions? Will the respondent be allowed documents or other memory aids during the interview? Is the respondent entitled to review or edit the interview transcript?
- Develop a protocol for the handling of classified sources and information.
- Arrange for transcription and translation assistance.
- Develop a protocol for making public information obtained from the interviews.

Because oversight can be complicated, it is usually helpful for the members of an oversight body, even when no requirement exists, to develop and agree to a common scenario prior to the start of the oversight activity. Detailed inspection plans, in particular, encourage commitment to the oversight process among the relevant stakeholders. Furthermore, the development of detailed procedures in advance makes it easier for members of an oversight body to concentrate on content once the inspection begins.

9. PROFESSIONALISM AND CREDIBILITY OF OVERSIGHT BODIES

Persons living in democratic societies expect their governmental agencies to comply with the laws of the country and, if they do not, to be held accountable by oversight bodies. Because of the exceptional powers that intelligence services possess—which can limit or violate human rights—the bodies that oversee those services have a correspondingly

great responsibility. Thus, it is incumbent upon them to demonstrate in their work and public demeanour the highest standards of oversight professionalism. Otherwise, the credibility of the oversight process will suffer, and the public will lose confidence in their governmental institutions.

9.1 INDEPENDENCE OF THE OVERSIGHT BODY

An oversight body cannot be considered professional if its independence and autonomy are not absolutely guaranteed by law. Professionalism also requires that oversight bodies be thoroughly non-partisan—that is, free from the pressures of party politics, executive meddling, and media pressure.

As a practical matter, the best way to defend against political or media pressure is to be mindful of it. For this reason, oversight personnel often benefit from media training, which, among other things, prepares them to answer unexpected questions from politicians or the media. This is particularly important in view of the need to prevent the inadvertent disclosure of confidential information when responding to such questions.

9.2 EXPERTISE OF OVERSIGHT EMPLOYEES

Ideally, members of oversight bodies and their employees should have prior knowledge of and experience with a range of security agencies, including police and military agencies as well as foreign and domestic intelligence services. Those who do not should receive training at the earliest possible opportunity and be encouraged and/or required to attend continuing education seminars on a regular basis, as well as to review the applicable rules and regulations.

9.3 CLASSIFIED INFORMATION

One of the most difficult professional dilemmas facing oversight personnel is how best to balance the competing demands of transparency and secrecy (see Nathan–Tool 3). Because disclosure of certain confidential information can indeed endanger national security, governments have a legitimate right to keep such information secret from the public at large. It is for this reason that employees of oversight bodies must first obtain security clearances before handling classified information. Yet too much secrecy is also undesirable, especially when over-classification is used to obscure politically embarrassing activities (such as, in the United States, the creation of secret detention, interrogation, and rendition programmes). Misuse of state secrecy laws can cause citizens to lose faith in their government, undermining the legitimacy of all governmental institutions. Furthermore, over-classification hampers effective oversight. (This problem is ameliorated in some jurisdictions by laws that empower the judiciary to review whether or not particular documents have been properly classified.)

10. CONDUCT OF OVERSIGHT BODIES

The manner in which an oversight body conducts itself can have a substantial impact on its effectiveness. If oversight bodies do not themselves embrace such values as transparency and consistency, they cannot legitimately expect intelligence services to do the same.

10.1 TRANSPARENCY

The effectiveness of an oversight body is best served by maximum transparency. In particular, it is essential that oversight bodies act in accordance with agreed-upon standards and protocols so that they can always explain their actions and demonstrate the accountability that they expect of the intelligence services they oversee. The transparency of an oversight body may be enhanced by the inclusion in its reports of information about sources consulted and terms of reference used for a particular investigation.

10.2 CONSISTENCY

Shocks or scandals typically produce intense bouts of intelligence oversight, followed by periods of rigorous monitoring. It is however, important that oversight occurs on an ongoing basis and not only in response to problems. Intelligence oversight bodies can promote greater consistency in their work by developing a pattern of monitoring and inspections. Such an approach helps to avoid inattentiveness or new gaps in oversight and ultimately reduces the likelihood of intelligence failures reoccurring.[24]

10.3 INTERACTING WITH INTELLIGENCE SERVICES

Even though intelligence services may appear to be closed, insular bureaucracies, most are reflective organizations willing to remedy their deficiencies. For this reason, oversight bodies have an interest in making their interactions with intelligence services engaging, timely, and instructive. For instance, specific recommendations for corrective action should be presented in ways that permit intelligence services to translate them into concrete guidelines, protocols, procedures, and timetables that make sense within their own organizations.

It is also important for oversight personnel to be mindful of the adverse effects their findings can have on individual intelligence officers, resulting often in their discipline and sometimes in their dismissal. For this reason, it is usually advisable for members of oversight bodies to discuss such matters with senior management at the relevant service before reporting their findings.

11. REPORTING

Although intelligence oversight bodies follow a wide range of reporting procedures, they are universally obliged to make known the results of their inquiries. In nearly all cases, the law requires them to submit reports on a regular basis, typically annually. Such reports generally include descriptions of investigations undertaken and, if within the oversight body's mandate, budgetary analysis. The reports can also include recommendations, addressed to the intelligence services and/or the executive, for improvement of service accountability, transparency, legality, and effectiveness.

Oversight bodies may also produce special reports throughout the year. These may be thematic or descriptive of a particular investigation. For example, should an oversight body become aware of questionable intelligence activity, it is generally required to report that activity in a timely manner to a relevant authority.

According to Aidan Wills, "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 their public reports. This consultation gives these services the chance to share any concerns they may have regarding the inclusion of sensitive information in the report."[25]

11.1 SUBMISSION OF REPORTS

Submission routines vary from country to country. In Belgium, Committee I sends its annual report to the presidents of both houses of Parliament and to the responsible minister. Special reports, however, are presented first to the responsible minister and only later to the president of the upper house of Parliament.[26] Furthermore, reports submitted to Parliament do not contain classified information. In Canada, where the reporting rules are different, SIRC submits its annual report to the executive, which must transmit the report to Parliament within fifteen days. SIRC is also required by law to consult with the CSIS director before making the report public.

11.2 OWNERSHIP OF REPORTS

Oversight bodies should have full ownership of their reports, including their content and timing. In some cases, laws or rules of procedure may dictate the special handling of classified information or a period of time before a report can be made public. In the Netherlands, the CTIVD allows the responsible minister six weeks. If no formal response is submitted by the relevant minister within those six weeks, the underlying report of the intelligence oversight body is published.

11.3 POLITICAL CONSIDERATIONS

Intelligence activity that takes place on the fringes of political legitimacy can be highly controversial. Examples include the gathering of intelligence within the jurisdiction of a foreign country and the use of special investigative measures that infringe on the human rights of individuals. Hence, oversight investigations often attract partisans eager to use oversight findings to their own political advantage. The best way to deal with these pressures is to anticipate them. Be aware, for instance, of the political calendar and its effect on the attention of journalists. Reflecting on the political consequences that will likely follow from a report can instruct its preparation. On the other hand, excessively orchestrating a report's disclosure can make an oversight body seem complicit rather than independently objective.

11.4 IMPLEMENTATION OF REPORTS

A report is not an end in itself. Rather, its purpose is to generate discussion of the matters being presented in the report within parliament, the government, and beyond. Only in this way can the findings of a report lead to the implementation of its recommendations.

Every oversight report, whether incidental or periodic, should list clearly its conclusions and its recommendations for change. These should be precisely worded and numbered. In addition, once a report has been submitted to the relevant authorities, the oversight

body should work with these authorities to develop an implementation schedule. Later, the oversight body should create and submit a follow-up report on the extent to which its recommendations have been implemented by the respective intelligence services.

11.5 ACCESSIBILITY OF REPORTS

Through the use of modern technologies such as the Internet, oversight bodies can now make their reports broadly accessible to members of the public. The UK inquiry into national involvement in the Iraq war (the Chilcot inquiry) has already published transcripts, witness statements, and other unclassified documents on its web site in preparation for the issuance of its final report.

It may be that the report of an oversight body is posted on a web site that the oversight body does not control—such as a ministerial or parliamentary web site. To ensure that its reports remain available to the public, the oversight body should insist that it be informed in advance whenever decisions are made to remove reports. It is therefore, recommendable that oversight bodies have permanent public web sites to provide easy access to reports and other documents.

12. POTENTIAL FINDINGS

Intelligence oversight bodies consider a wide range of matters, some of which are general (such as a service's legislative framework) and others of which are specific (such as the investigation of a particular incident). Below are examples of three potential findings that may result from oversight investigations. Each discusses recommendations for improvement that might follow from them.

12.1 AN INTELLIGENCE SERVICE FAILED TO VERIFY INFORMATION PROVIDED BY FOREIGN PARTNERS

Especially when acting in cooperation with foreign partners, intelligence services may fail to verify properly information that they receive from outside sources. In 2009 in the Netherlands, for instance, the CTIVD investigated the use of foreign intelligence by the General Intelligence and Security Service (GISS), finding that the GISS often failed to determine, as required by law, whether a foreign intelligence service qualified for cooperation. According to the CTIVD's final report, "No structured decision-making process was found." Instead, the report continued, "decisions were often made on an *ad hoc* basis," which the CTIVD criticized as "too limited" and "undesirable." The GISS was therefore advised to begin making well-considered assessments, not only when entering into a cooperative relationship but also with regard to already established relationships.[27]

Making such assessments before acting on supplied intelligence is particularly important when the supplied information may have been obtained through torture. For this reason, the Canadian Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar recommended that all foreign liaison agreements be routinely subjected to scrutiny by oversight bodies.[28] The UN special rapporteur has similarly recommended that countries include in their intelligence-sharing agreements a clause that makes the application of such agreements subject to scrutiny by their respective review bodies and which declares that those review bodies are competent to cooperate with one another

in assessing the performance of either or both parties.[29] (For further discussion of information sharing, please see Roach—Tool 7).

12.2 AN INTELLIGENCE SERVICE ACTED BEYOND ITS MANDATE

Oversight bodies must regularly consider whether the activities of an intelligence service exceed its mandate, especially with regard to the use of special powers to collect information (see Hutton–Tool 5). If the intelligence service has indeed failed to respect the legal limits of its authority, the oversight body must hold the service accountable. This can be accomplished by reporting the violation to the relevant authorities and, if within the oversight body's own mandate, terminating the use of one or more of the service's special powers.

The Arar commission, after establishing inter alia that the RCMP had exceeded its mandate, recommended that the RCMP henceforth respect the distinct role of the CSIS within the Canadian intelligence community.[30]

12.3 INTELLIGENCE HAS BEEN POLITICIZED

Intelligence can become politicized in a number of ways, not all of which involve the intelligence service producing the intelligence. Most commonly, however, politicization results from an overly intimate relationship between the executive and service officials who consciously or unconsciously tailor intelligence to support established executive positions ("intelligence to please"). A related form of politicization involves the use of intelligence services by government officials to obtain damaging information on their political opponents. Politicization can also arise within an intelligence service from rival analysts competing to produce actionable intelligence in order to advance their careers.

An oversight body encountering evidence of intelligence politicization should recommend that parliament debate openly the proper objectives of foreign and defence policy. It should also consider what safeguards might be introduced to prevent the future use of intelligence as a political instrument.[31]

13. RECOMMENDATIONS

- The mandate of an intelligence oversight body should be defined in a formal, detailed manner, preferably as part of a comprehensive legislative framework covering the oversight of all intelligence services.
- If the mandate of an intelligence service is changed, the mandate of its oversight body should be revised accordingly.
- Taken together, the mandates of a nation's intelligence oversight bodies should cover its entire intelligence community, including civilian and military services as well as supporting departments and officials.
- The powers of access, investigation, inspection, and approval included in an intelligence oversight body's mandate should be commensurate with the powers of the intelligence services that the body oversees.

- An intelligence oversight body should have the authority to inspect sites, hold open and closed hearings, and access classified information in documents, databases, and other computer files.
- An intelligence oversight body should be able to conduct *ex post* oversight. In the exceptional case, where an intelligence oversight body performs *ex ante* oversight, members should be vetted by a security agency to ensure that source identities and other operational information are protected.
- In order to organize its work and encourage commitment from relevant stakeholders, an intelligence oversight body should always create an oversight plan.
- An intelligence oversight body should maintain a high standard of professionalism. This enhances not only the legitimacy of the oversight body but also, indirectly, the legitimacy of the intelligence services it oversees.
- The conduct of an intelligence oversight body should be transparent, consistent, and accountable.
- An intelligence oversight body should publish periodic (annual) reports describing its activities and findings. It should also publish, as appropriate, incidental reports describing specific investigations.
- The reports of an intelligence oversight body should be broadly accessible by the public.
- An intelligence oversight body should submit its draft findings to the senior management of the intelligence services for their response within a legally mandated period of time.
- Reports of an intelligence oversight body should always include recommendations that can be implemented by the intelligence services concerned.
- An intelligence oversight body should actively monitor the implementation of its recommendations and publish follow-up reports.

Endnotes

1. Marina Caparini, "Controlling and Overseeing Intelligence Services in Democratic States," in *Democratic Control of Intelligence Services: Containing Rogue Elephants*, eds. Hans Born and Marina Caparini (Aldershot, UK: Ashgate, 2007), p. 12.
2. Committee on Foreign Affairs, 26 September 2003, 03-BuZa-61.
3. In the interest of social legitimacy, intelligence services should also act in accordance with the public interest. Specifically, they should refrain from invading the privacy of individual citizens in an unfounded, disproportionate, and/or illegal manner.
4. Tommaso F. Giupponi and Federico Fabbrini, "Intelligence agencies and the State secret privilege: the Italian experience," *International Constitutional Law Journal* Vol. 4, No. 3 (Fall 2010), pp. 443–466 (available at http://www.internationalconstitutionallaw.net/download/53c4319b67f44d52a392c655f17245a3/Giupponi_Fabbrini.pdf; accessed 19 July 2011).
5. Special investigative measures include the interception of communications, the running of informants and infiltrators, and the construction of façades.
6. Canadian Security Intelligence Service web site, "Accountability and Review" (available at http://www.csis-scrs.gc.ca/bts/ccntblt-eng.asp; accessed 17 August 2011).
7. It is generally recommended that a nation's entire intelligence community be subjected to the oversight of at least one parliamentary committee.
8. Australian Department of the Prime Minister and Cabinet web site, *Report of the Inquiry into Australian Intelligence Agencies*, Chapter 4 (available at http://www.dpmc.gov.au/publications/intelligence_inquiry/chapter4/oversight.htm; accessed 17 August 2011).
9. Hans Born, "Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices," *Quarterly Journal* Vol. 3, No. 4 (December 2004), p. 6 (available at http://www.pfpconsortium.org/file/1645/view; accessed 19 July 2011).
10. Guy Rapaille, "Le Comité permanent R dans un rôle d'organe juridictionnel: Le nouveau rôle du Comité belge dans le cadre du contrôle des methods particulières de recueil de données" (speech at the 6th Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the European Union Member States, Brussels, 30 September–1 October 2010) (available at http://www.parlement-eu2010.be/pdf/30sep-1okt-Thema0-Guy-Rapaille.pdf; accessed 18 July 2011).
11. For example, see United Kingdom, Intelligence and Security Committee, *Annual Report 2010–2011*, Cm 8114 (2011) (available at http://www.cabinetoffice.gov.uk/sites/default/files/resources/isc-annualreport1011.pdf; accessed 13 October 2011).
12. Sandy Africa, "The South African Intelligence Services: A Historical Perspective," in *Changing Intelligence Dynamics in Africa*, eds. S. Africa and J. Kwadjo (Birmingham, UK: Global Facilitation Network for Security Sector Reform/African Security Network, 2009), pp. 61–94.
13. For a discussion of this point, see Paul Robinson, *Eyes on the Spies: Reforming Intelligence Oversight in Canada*, Centre for International Policy Studies (CIPS) Policy Brief No. 1 (Ottawa: CIPS, University of Ottawa, November 2008) (available at http://www.sciencessociales.uottawa.ca/cepi-cips/eng/documents/CIPS_PolicyBrief_Robinson_Nov2008.pdf; accessed 17 August 2011).
14. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (2006), p. 351 (available at http://www.sirc-csars.gc.ca/pdfs/cm_arar_rcmpgrc-eng.pdf; accessed 17 August 2011).
15. Iraq Inquiry web site, "About the Inquiry" (available at http://www.iraqinquiry.org.uk/about.aspx; accessed 18 August 2011).
16. For a discussion of the Norwegian system of intelligence oversight, which takes this approach, see Trygve Harvold, "Norwegian Parliamentary Oversight: an 'effective remedy'?" (speech at the 6th Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the European Union Member States, Brussels, 30 September–1 October 2010) (available at http://www.parlement-eu2010.be/pdf/30sep-1okt-Thema1-Trygve%20Harvold.pdf; accessed 18 July 2011).
17. Hans Born, "Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices," *Quarterly Journal* Vol. 3, No. 4 (December 2004), p. 9 (available at http://www.pfpconsortium.org/file/1645/view; accessed 19 July 2011).
18. United Nations Human Rights Council, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, United Nations Document A/HRC/10/3 (4 February 2009), p. 24 (available at

http://www.unhcr.org/refworld/pdfid/49b138c32.pdf; accessed 18 August 2011).

19. Hans Born, "Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices," *Quarterly Journal* Vol. 3, No. 4 (December 2004), p. 3 (available at http://www.pfpconsortium.org/file/1645/view; accessed 19 July 2011).
20. Australian Department of the Prime Minister and Cabinet web site, *Report of the Inquiry into Australian Intelligence Agencies*, Chapter 8, Recommendation 22 (available at http://www.dpmc.gov.au/publications/intelligence_inquiry/chapter8/1_findings.htm; accessed 17 August 2011).
21. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), Chapter 9 (available at http://www.sirc-csars.gc.ca/pdfs/cm_arar_rec-eng.pdf; accessed 19 October 2011).
22. For a discussion of this inquiry, see Parlement & Politiek web site, "Parlementaire enquête opsporingsmethoden, IRT (1994-1996)" (available at http://www.parlement.com/9291000/modulesf/g8pdkcx4; accessed 19 July 2011).
23. This summary is derived from a sample plan presented in United States Army Inspector General School, *Intelligence Oversight Guide* (February 2008), Appendix D (available at http://www.fas.org/irp/doddir/army/ioguide.pdf; accessed 15 July 2011).
24. Loch K. Johnson, *Secret Spy Agencies and a Shock Theory of Accountability*, Department of International Affairs Occasional Papers (University of Georgia, School of International and Public Affairs, 2006) p. 2.
25. Aidan Wills, *Guidebook: Understanding Intelligence Oversight*, Toolkit—Legislating for the Security Sector (Geneva: DCAF, 2010), p. 40.
26. Ibid., p. 37.
27. Bert van Delden, "Partners in Business?" (speech at the 6th Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the European Union Member States, Brussels, 30 September–1 October 2010), p. 4 (available at http://www.parlement-eu2010.be/pdf/30sep-1okt-Thema3-Bert%20Van%20Delden.pdf; accessed 18 July 2011).
28. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (2006) (available at http://www.sirc-csars.gc.ca/pdfs/cm_arar_rcmpgrc-eng.pdf; accessed 17 August 2011).
29. United Nations Human Rights Council, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, United Nations Document A/HRC/10/3 (4 February 2009), p. 21 (available at http://www.unhcr.org/refworld/pdfid/49b138c32.pdf; accessed 18 August 2011). In reference to C. Forcese, *The Collateral Casualties of Collaboration: the Consequence for Civil and Human Rights of Transnational Intelligence Sharing* (conference paper for the DCAF workshop on accountability of international intelligence cooperation, Oslo, 17 October 2008).
30. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (2006), p. 312 (available at http://www.sirc-csars.gc.ca/pdfs/cm_arar_rcmpgrc-eng.pdf; accessed 17 August 2011).
31. For a further discussion, see Monica den Boer, "Keeping 'Spies & Spooks' on the Right Track: Ethics in the Post 9/11 Intelligence Era," in *Ethics and Security*, eds. Monica den Boer and Emile Kolthoff (The Hague: Eleven, 2010), pp. 57–83.

TOOL 5

Overseeing Information Collection

Lauren Hutton

5

Overseeing Information Collection

Lauren Hutton

1. INTRODUCTION

The purpose of this tool is to examine the role that oversight bodies play in monitoring the information-collection functions of intelligence services. The production of intelligence is a multistep process, requiring tasking, planning, information collection, analysis, and dissemination. Yet of all these steps, it is the collection of information, especially through secret means, that remains the defining characteristic of intelligence services, at least in the public mind. Information collection is one of the most controversial aspects of intelligence work, and it presents an unusual set of challenges to oversight bodies charged with upholding democratic ideals.

The first part of this tool will consider some of the methods by which intelligence services gather information. It will then look at ways in which democratic countries can use legislation, authorization, and oversight to ensure that human rights are respected whenever secret methods are employed.

2. INFORMATION COLLECTION SOURCES AND METHODS

The basis of intelligence is information collected from various sources. Because no single source is likely to provide enough information for a full understanding of a particular

issue, intelligence services use multiple sources to arrive at the most accurate picture of events. These sources are usually categorized by type:

- human intelligence (HUMINT), such as informants
- signals intelligence (SIGINT), such as communications intercepts
- open-source intelligence (OSINT), such as media reporting
- imagery intelligence (IMINT), such as satellite photographs

Methods for collecting information can be overt or covert. Overt methods are most often used to gather OSINT because that information is openly held and publicly available. Covert, or clandestine, methods of information collection use secrecy to gather information about targets without the knowledge of the targets. Covert methods can include the use of informants, electronic surveillance, interception of communications, physical surveillance, and remotely collected images. When such methods are used in a manner that infringes on an individual's right to privacy, they are called "intrusive methods of investigation." The techniques themselves are called "special investigative measures" or "special investigative techniques."

The Council of Europe has defined *special investigative techniques* to mean "techniques applied by the competent authorities in the context of criminal investigations for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target persons."[1] In this context, *competent authorities* can mean either intelligence services or law-enforcement agencies. It is important to note that, in many countries, intelligence services use such measures not only in the context of criminal investigations but also in preventive, national security investigations. As a general principle, the method used to gather information should be based on the type of information required, the purpose of the collection effort, and the operational, legal, and political context in which the intelligence services operate.

3. IMPACT OF INFORMATION COLLECTION ON HUMAN RIGHTS

Intelligence services collect information to assist executive officials in making policy and in taking strategic and operational decisions. The way they collect information should be consistent with the priorities and values of the society they serve.[2] In democratic countries, intelligence services should respect human rights, the rule or law, and the principles of democratic governance including accountability, transparency, and participatory decision making. The intelligence process from tasking through dissemination should operate within these parameters.

The gathering of information about security threats can directly impact the fundamental rights of individuals.[3] According to the 2008 report of the South African Ministerial Review Commission on Intelligence, which investigated suspected abuses of power by the National Intelligence Agency, "intrusive methods of investigation can play a crucial role in uncovering criminal activities and conspiracies but they can also be misused to subvert the democratic process, interfere with lawful political and social activity and create an unfair advantage for some politicians and parties."[4]

While use by the state of intrusive methods is always constitutionally and politically sensitive, their use by intelligence services should be treated with particular caution. The reasons for this caution, enumerated in the Ministerial Review Commission's report,[5] include the following:

- The target of an investigation may never learn of the use of intrusive methods and therefore may not be able to object to them nor challenge their validity in court.
- The high level of secrecy surrounding intrusive methods reduces the ability of oversight bodies to monitor their use and detect possible abuses and illegalities.
- The extent to which intrusive methods violate an individual's right to privacy may be far greater than is necessary or intended.
- Beyond infringing on a target's privacy, intrusive methods often encroach on the privacy rights of individuals with whom the target has contact, even though these individuals are not subjects of the investigation.
- Sensitive information about the target and the people with whom the target has contact is recorded and retained by the intelligence service beyond the time period of the investigation and sometimes used for other purposes.

A distinction is sometimes made between foreign and domestic uses of interception technology, because domestically there exists the danger that the executive will use clandestine interception systems for partisan purposes, such as to spy on political opponents. The interception of foreign communications, on the other hand, generally does not endanger the domestic democratic order.

In democratic countries, intelligence oversight bodies have a legitimate right and often a legal responsibility to ensure that intelligence services conduct themselves in a manner consistent with the constitutional order. Oversight bodies usually have a scope of responsibility that extends to the entire intelligence process, but the area of information collection requires special attention because of the dangers that covert, intrusive methods pose to democratic values. Specifically, oversight bodies should monitor closely the use of all such methods to ensure that intelligence service conduct remains within the boundaries of the law.

3.1 PROTECTING THE RIGHT TO PRIVACY

The right most often restricted or violated by intelligence services is the right to privacy. Accordingly, a key function of intelligence oversight bodies should be to ensure that services collect information in a manner that complies with national and international law on the right to privacy.

The UN special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has defined the right to privacy as "the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others and free from State intervention and free from excessive unsolicited intervention by other uninvited individuals."[6]

Similarly, Article 17 of the International Covenant on Civil and Political Rights states that:

1. *No one shall be subjected to arbitrary or unlawful interference with his privacy,*

family, home or correspondence, or to unlawful attacks on his honour and reputation.

2. *Everyone has the right to the protection of the law against such interference or attacks.*

With 167 signatories, the International Covenant on Civil and Political Rights forms the basis for international law on the right to privacy. Because it holds privacy to be a fundamental human right, government actions that limit this right must be authorized by national law for a specific, legitimate purpose.

As established by the European Court of Human Rights, the protection of national security is a legitimate purpose for the limitation of a human right such as the right to privacy. However, according to the court, any such limitation must be imposed in accordance with national law, which must include safeguards against abuse and remedies should abuses nevertheless occur.[7]

The use of covert, intrusive information-collection methods by an intelligence service constitutes a limitation on the right to privacy. Therefore, all such uses need to be authorized by national law and employed only for specific, legitimate purposes. In South Africa, the former inspector general for intelligence interpreted this principle as follows:

> *A limitation of rights may be justified on grounds of threats to national security. Such limitation should meet the test of proportionality which includes the nature of the right and the importance of the purpose of the limitation. As such the capacity to gather intelligence should be matched by equally strong safeguards that protect the constitutional rights of citizens and sustain an open and democratic society.*[8]

3.2 IMPACT OF TECHNOLOGY ON INFORMATION COLLECTION

Modern information and communications technology makes it possible for individuals all over the world to communicate instantly with one another and for information to travel great distances in an instant. However, it also enables governments to conduct an unprecedented degree of surveillance. Using advanced technological devices, intelligence services can collect information on a mass scale, gathering much more information than they can possibly absorb and analyze. Because this information collection is, by its nature, indiscriminate, it has the potential to violate human rights and should be undertaken only within a legal framework that protects the right to privacy.

The ECHELON Interception System provides a useful example. This system—operated jointly by the United States, the United Kingdom, Australia, Canada, and New Zealand as part of a collective security arrangement—intercepts signals passing to and from orbiting satellites. In 2000, the European Parliament created a temporary committee to investigate the potential impact of the ECHELON system on individuals' rights under European Union (EU) law. The committee's final report concluded that mass interception systems such as ECHELON have the potential to violate the right to privacy because they do not comply with the principle of proportionality with regard to the use of intrusive methods. While acknowledging that such interception systems may be justified on national security grounds, the committee recommended that their use be governed by clear and accessible legislation and that EU member states establish rigorous oversight.[9]

4. LEGAL FRAMEWORKS FOR INFORMATION COLLECTION

In most democratic countries, the collection of information by intelligence services is governed by a legal framework that ensures accountability and transparency. This is typically done by removing authorization and oversight responsibilities from the exclusive purview of the executive and sharing them (to various degrees) among the parliament, the judiciary, and other non-executive entities.

International law can inform the development of national law. For example, in 2005, the Council of Europe issued the following recommendations for the creation of national legislation on the use of special investigative techniques in criminal investigations:[10]

1. *Member states should, in accordance with the requirements of the European Convention on Human Rights (ETS No. 5), define in their national legislation the circumstances in which, and the conditions under which, the competent authorities are empowered to resort to the use of special investigation techniques.*
2. *Member states should take appropriate legislative measures to allow, in accordance with paragraph 1, the use of special investigation techniques with a view to making them available to their competent authorities to the extent that this is necessary in a democratic society and is considered appropriate for efficient criminal investigation and prosecution.*
3. *Member states should take appropriate legislative measures to ensure adequate control of the implementation of special investigation techniques by judicial authorities or other independent bodies through prior authorization, supervision during the investigation or ex post facto review.*

In general, national legislation concerning the use of covert, intrusive methods of information collection should specify:

- when such methods can be used.
- what threshold of suspicion needs to be met.
- what restrictions and limitations apply.
- what authorizations are required.

Examples of specific national legislation governing the domestic use of covert, intrusive information-collection methods include the Australian Telecommunication Interception and Access Act, the Australian Communications Assistance to Law Enforcement Act, the US Foreign Intelligence Surveillance Act, and the UK Regulation of Investigatory Powers Act. Any such law should address these three key issues:

- permissible objectives
- proportionality
- authorization and oversight

More generally, they should require competent authorities to be reasonably certain that covert, intrusive methods will yield the information sought.

4.1 PERMISSIBLE OBJECTIVES

Permissible objectives for the use of covert, intrusive methods of information collection

differ significantly from state to state. In some countries, as recommended by the Council of Europe, pursuit of a criminal investigation is a permissible objective.[11] In others, protecting national security and defending the democratic order are also permissible objectives. Section 3 (1) of the German Act Restricting the Privacy of Correspondence, Posts, and Telecommunications empowers the German government (i.e., the security services including police and intelligence services) to order restrictions on an individual's right to privacy if "concrete indications give rise to the suspicion that a person is planning, committing or has committed" a crime against:

- peace
- the democratic order
- national security
- the security of troops stationed in Germany

The term *concrete indications* establishes a high threshold that must be met before covert, intrusive methods can be employed. In order to ensure that there are significant reasons for the use of intrusive methods of investigation, such justification should be included in the application for authorization.

4.2 PROPORTIONALITY

Legislation governing the use of covert, intrusive methods of information collection should require that the degree of intrusion be proportional to the objective of the investigation. In this regard, the Council of Europe has recommended that special investigative techniques be used only when:

- there is probable cause to believe that a serious crime has been committed or is being planned.
- due consideration has been given to the "proportionality between the effects of the use of special investigation techniques and the objective that has been identified."[12]

The Council has further recommended that member states use less intrusive methods whenever "such methods enable the offence to be detected, prevented or prosecuted with adequate effectiveness."[13] Guidelines such as these enable the use of intrusive methods for legitimate purposes while keeping abuse and infringement of human rights to a minimum.

The principle of proportionality is more difficult to apply in relation to threats to national security. The primary goals should be to ensure that the information collected through intrusive methods could not have been collected through less intrusive methods and that the use of the intrusive method can yield the information sought. For example, in Germany, an order to use collection methods that limit the right to privacy may only be issued "where the use of another method to investigate the facts would be futile or render the investigation significantly more difficult."[14]

4.3 AUTHORIZATION AND OVERSIGHT

To prevent abuse of covert, intrusive information-collection methods, legal frameworks should include both authorization procedures (involving senior intelligence service management and the judiciary) and oversight mechanisms (involving the parliament and expert oversight bodies). Appropriate structures for authorization and oversight will be

discussed in detail in the next two sections. These levels of authorization and oversight are not mutually exclusive, and a comprehensive and robust system for accountability and transparency could include more than one level of authorization and more than one mechanism of oversight.

5. AUTHORIZATION OF INFORMATION-COLLECTION OPERATIONS

Different types of information-collection operations require different degrees of authorization. For example, physical surveillance, although covert, is not highly intrusive; therefore, an internal intelligence service authorization is usually sufficient. Tapping a telephone, however, or intercepting mail represents a greater infringement on a reasonable expectation of privacy and thus should require a higher level of authorization, such as from the minister responsible for intelligence and/or from a judge. Any renewal of collection operations should involve the same level of authorization as the original request.

5.1 INTERNAL AUTHORIZATION

Requiring the senior management of an intelligence service to authorize the use of special investigative techniques establishes accountability within the service and provides an important deterrent to misconduct. Although this requirement may not be sufficient in and of itself to prevent abuse, it signifies that choosing to limit an individual's right to privacy is a serious, weighty decision, not to be taken lightly. Within a service, decision-making authority should be structured so that the greater the invasion of privacy, the higher the level of authorization needed.

5.2 EXECUTIVE AUTHORIZATION

Intelligence services are controlled by the executive, which sets their priorities and directs their activities. This is normally the responsibility of a designated minister. The same minister may also be responsible for authorizing specific information collection operations. Just as internal authorization requirements ensure that senior service management can be held to account for their use of special investigative techniques, so do executive authorization procedures for the responsible minister's decision to approve particular measures.

Abuse on the ministerial level most often involves the use of an intelligence service's information-collection apparatus to gather confidential information about political opponents of the government. For this reason, with respect to the domestic use of covert information-collection methods, legal frameworks should include authorization procedures that:

- establish limits on what ministers can ask services to do.
- require judicial authorization for the use of intrusive methods of information collection in addition to ministerial authorization.
- create a mechanism by which intelligence officers can report misconduct.
- establish or designate an independent oversight body to review the conduct of such operations.

5.3 JUDICIAL AUTHORIZATION

In most democratic countries, a traditional responsibility of the judiciary is to protect the human rights of individuals. Given this role, it makes sense for judges to be given the task of weighing the protection of human rights against the information-collection needs of the intelligence services. It is common practice, therefore, for national law to require intelligence services to obtain judicial authorization (usually in the form of a warrant) before infringing on an individual's right to privacy. Such warrants, because they are the product of an impartial evaluation, are considered to be an important check on potential abuse.[15] Furthermore, as noted in the Venice Commission report on democratic oversight of security services, judicial authorization requirements subordinate security concerns to the law and thereby institutionalize respect for the law.[16]

It is good practice for governing legislation to specify the type of operations that require judicial authorization, as well as what authority the judge may have to limit the scope, duration, and targets of an operation. Legislation should also set minimum information requirements for any warrant application (see Box 1).

Box 1: Application requirements for judicial authorizations in Canada

The Canadian Security Intelligence Service Act requires that intelligence service applications for judicial communication-interception warrants include the following information:[17]

- the facts relied on to justify the belief that a threat to national security exists
- evidence that less intrusive techniques have been tried and have failed or reasons why they are unlikely to succeed
- the type of communication to be intercepted
- the type of information to be obtained
- the identity of the persons or classes of persons who are the targets of the investigation
- the identity of the persons, if known, whose communications will be intercepted
- a general description of the place, if known, where the warrant will be executed
- the period for which the warrant is being requested
- the details of any previous application made in relation to a person identified in the current application—including the date of the previous application, the name of the judge to whom the previous application was made, and the decision of the judge thereon

In many countries, a judicial warrant is required for the interception of communications. The National Intelligence Law of Argentina, for example, requires the country's intelligence services to obtain judicial authorization before intercepting private communications of any type.[18]

Governing law sometimes provides for intelligence service applications to be heard by specialist judges. Canada, France, South Africa, and Spain, among other nations, follow this practice. Alternatively, some countries have created special courts to provide judicial authorization. Among these is the US Foreign Intelligence Surveillance Court (FISC), established by the Foreign Intelligence Surveillance Act of 1978. Comprised of eleven federal district court judges serving staggered, non-renewable terms of no more than seven years, the FISC reviews applications for warrants on matters of national security. The act also established the Foreign Intelligence Surveillance Court of Review, which hears government appeals of FISC decisions.[19]

Sometimes, these specialist judges and courts have the authority to review information-collection operations while they are under way. In South Africa, the Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002 enables judges to request interim written reports on the progress being made towards achievement of the objectives stated in the warrant.[20] In this way, they can limit collateral intrusion on unintended targets and ensure that covert, intrusive methods are not employed longer than is necessary.

6. OVERSIGHT OF INFORMATION-COLLECTION OPERATIONS

An important companion to authorization is oversight, which includes the review of intelligence service operations to confirm that they have been properly authorized. Only when both of these safeguards, authorization and oversight, are present can information-collection operations be considered effectively regulated. (For a discussion of the handling by oversight bodies of complaints against intelligence services, see Forcese—Tool 9)

Oversight can be performed by many different entities. Some, such as supreme audit institutions and national ombuds institutions, have relevance by virtue of their broad mandates. Others, such as inspectors general and expert oversight bodies, have specialized expertise that supports their specific mandates. Most countries divide oversight among several entities, with jurisdictions that overlap to varying degrees.

6.1 PARLIAMENTARY OVERSIGHT BODIES

Within democratic systems of government, parliaments are responsible for establishing the legal frameworks within which governmental bodies operate. They also have the responsibility to monitor compliance with the laws they enact. These responsibilities apply to intelligence services just as they do to any government agency.

However, because intelligence services differ in many ways from other government agencies, parliaments typically create intelligence oversight committees to monitor service activity and recommend revisions to the legal frameworks within which they operate. With respect to information-collection operations, these committees are usually charged with:

- overseeing the use of covert, intrusive methods
- monitoring the budgeting and use of funds
- scrutinizing the legal framework to ensure that it contains sufficient safeguards to protect human rights
- ensuring that the intelligence services comply with the legal framework

Additionally, governing law can empower parliamentary committees to review covert, intrusive information-collection operations. Notably, parliamentary oversight committees can play an essential role in ensuring that authorization procedures have been correctly applied. For example, the National Intelligence Law of Argentina empowers the Joint Committee for the Oversight of Intelligence Agencies and Activities to compel the preparation (and presentation to the committee) of reports listing "the intercepts and taps that have been performed in a given period."[21] The committee can then use this list

to check the use of special investigative techniques against approvals granted. In this way, it can confirm that authorization procedures are being administered properly; see Box 2 below for example.

Box 2: Parliamentary oversight of information collection in Germany

In Germany, the use of intrusive information-collection methods is overseen by the Parliamentary Control Panel.

The law requires the executive to furnish the control panel with reports on the use of intrusive methods "at intervals of no more than 6 months." Based on these periodic reports, the panel prepares an annual report for the Bundestag on the nature and scope of the intrusive methods employed under the act.[22]

In addition to this monitoring function, the act also gives the control panel an authorization role. The Federal Intelligence Service (a foreign intelligence service) must obtain the approval of the control panel before it can intercept international telecommunications traffic that is transmitted in "bundled form" and may have connection with Germany or German nationals. These are interceptions based on key words, which do not target specific communications.[23]

Membership in a parliamentary oversight committee does not generally require any intelligence expertise. However, as one member of the US Congress has observed, in order to reach appropriate judgments, committee members must familiarize themselves with the intelligence being produced and the methods used to produce it.[24]

6.2 EXPERT OVERSIGHT BODIES

Expert intelligence oversight bodies are independent entities whose members and staffs possess particular intelligence expertise (see Born and Geisler Mesevage–Tool 1). One of the most common types of expert oversight body is inspectors general. Although their functions and responsibilities vary from state to state, inspectors general are normally independent entities authorized to receive and act on complaints concerning the legality of intelligence service conduct. Their mandates usually include the right to conduct investigations into the use of special investigative techniques and covert collection methods. In some countries, such as the United States and Canada, they operate within the intelligence services. In others, such as South Africa, they are independent of the intelligence services.

The South African inspector general for intelligence has these primary oversight responsibilities:[25]

- reviewing the activities of the intelligence services to determine whether their conduct is lawful and their performance effective
- certifying the legality of intelligence service operations to the executive and the people of South Africa
- functioning as an ombuds institution with respect to complaints against intelligence services made by government officials and members of the public

In contrast, Belgium (see Box 3), Germany (see Box 4), Norway, and the Netherlands use expert bodies to oversee their intelligence services. With respect to information-collection operations, these expert bodies perform the following tasks:

- ensuring that the operations comply with the legal framework, internal service procedures, and executive policies
- monitoring operational effectiveness and making recommendations for its improvement
- handling complaints relating to the illegal use of special investigative techniques made by government officials and members of the public

Box 3: Belgium's Standing Intelligence Agencies Review Committee

An example of an expert oversight body is Belgium's Standing Intelligence Agencies Review Committee, established by the Act Governing the Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment. The committee is mandated to oversee the functioning of Belgium's two intelligence services and the Coordination Unit for Threat Assessment. The committee's oversight focuses on legality and effectiveness of the intelligence services' activities, as well as the coordination of the intelligence and security community. In order to meet these responsibilities, the committee is empowered to "investigate the activities and methods of the intelligence services," including the ways in which the services collect information.[26]

In 2010 the committee was given the task of supervising the intelligence services' use of newly acquired intrusive intelligence-collection methods. The committee evaluates each intrusive surveillance operation and may order its termination (and the destruction of information collected) if it does not comply with the law.[27] Furthermore, the committee is authorized to handle "complaints and denunciations…with regard to the operation, the intervention, the action or the failure to act of the intelligence services."[28]

Box 4: Germany's G10 Commission

The expert oversight body that monitors information collection in Germany is the G10 Commission. The commission is comprised of four members, one of whom is a judge, and can include parliamentarians. Although the commissioners are appointed by the Parliamentary Control Panel, their independence in office is guaranteed by law. One of their main functions is deciding whether the use of intrusive collection methods by the intelligence services is permissible and necessary. Accordingly, the law requires the German government to brief the commissioners each month on upcoming operations that will employ intrusive methods of investigation. Should the commissioners declare any of these methods unnecessary or impermissible, the government must revoke its authorization for the operations.[29]

The G10 Commission also has a complaint-handling function. It can hear complaints concerning, inter alia, the use of intrusive information-collection methods and to decide whether those complaints merit limiting the ability of the intelligence services to use such methods.[30]

In order to be effective in overseeing information collection, an expert oversight body must have a mandate that allows it to be proactive. Specifically, it should be empowered to

conduct investigations on its own initiative and have access to a wide range of intelligence service information, whether classified or not. In turn, it should provide recourse for persons alleging infringements of their rights; and it should prepare regular reports for the parliament. (Redacted versions of these reports should be made public in order to promote transparency.)

7. CONCLUSION

This tool has examined when and how intelligence services should be allowed to limit human rights in order to achieve their security objectives. In other words, it has considered the question: When can public resources be used to limit the rights of individuals? Fundamental to this question is the relationship between citizens and their government. Whatever answer a society reaches, a rigorous and clearly defined system of authorizations and oversight is always necessary to ensure that intelligence agencies conduct themselves with the parameters of governing law.

Oversight of information-collection operations is particularly important because, in democratic countries, effective intelligence gathering depends on institutional legitimacy, credible governance, and ultimately public trust. These conditions can be achieved only if the activities of the intelligence services are rooted in and comply with legal frameworks that protect human rights and embrace the democratic principles of openness, transparency, and accountability. On these foundations, and only on these foundations, can the legitimate use of covert, intrusive methods be assured.

8. RECOMMENDATIONS

- The permissible uses of investigative methods that limit human rights, including the right to privacy, should be defined clearly in the legal framework within which the intelligence services operate.
- The legal framework should specify proper grounds for the use of covert, intrusive methods of information collection, recognizing that such methods should be used only when they are proportionate to the objective being sought and no other methods will suffice.
- The legal framework should create clear authorization procedures regulating the use of covert, intrusive methods of information collection. Greater degrees of intrusion should require higher levels of authorization.
- The legal framework should require judicial authorization for the domestic use of covert, intrusive methods of information collection. It should also establish procedures for designating the judges authorized to grant such approvals and determine what criteria they should use in evaluating government applications.
- The legal framework should create effective oversight mechanisms to monitor the use of covert, intrusive methods of information collection through parliamentary committees, expert oversight bodies, or both.

Endnotes

1. Council of Europe, Committee of Ministers, *Recommendation Rec(2005)10 of the Committee of Ministers to member states on "special investigation techniques" in relation to serious crimes including acts of terrorism* (20 April 2005), Rec(2005)10, Chapter I (available at https://wcd.coe.int/ViewDoc.jsp?id=849269&Site=CM).
2. For a fuller discussion of this point, see Ronnie Kasrils, "*To spy or not to spy? Intelligence and democracy in South Africa*," in To spy or not to spy? Intelligence and democracy in South Africa, ed. Lauren Hutton (Pretoria: Institute for Security Studies, 2009), pp. 9–22.
3. For a fuller discussion of this point, see Marina Caparini, "Controlling and Overseeing Intelligence Services in Democratic States," in *Democratic Control of Intelligence Services: Containing Rogue Elephants*, eds. Hans Born and Marina Caparini (Aldershot, UK: Ashgate, 2007), pp. 3–24.
4. South Africa, Ministerial Review Commission on Intelligence, *Intelligence in a Constitutional Democracy: Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP* (10 September 2008) (available at http://www.ssronline.org/document_result.cfm?id=3852; accessed 11 July 2011).
5. Ibid., pp. 158–159.
6. United Nations Human Rights Council, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, United Nations Document A/HRC/10/3 (4 February 2009), p. 6–7 (available at http://www.unhcr.org/refworld/pdfid/49b138c32.pdf; accessed 14 February 2012).
7. Council of Europe, European Commission for Democracy through Law (Venice Commission), *Report on the democratic oversight of the security services*, CDL-AD(2007)016 (2007) (available at http://www.venice.coe.int/docs/2007/CDL-AD%282007%29016-e.asp; accessed 22 October 2011).
8. South Africa, Ministerial Review Commission on Intelligence, *Intelligence in a Constitutional Democracy: Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP* (10 September 2008), p. 157 (available at www.ssronline.org/document_result.cfm?id=3852).
9. European Parliament, Temporary Committee on the ECHELON Interception System, *Draft document on the existence of a global system for intercepting private and commercial communications (ECHELON interception system)* (2001) (available at http://cryptome.org/echelon-ep.htm; accessed 16 July 2011).
10. Council of Europe, Committee of Ministers, *Recommendation Rec(2005)10 of the Committee of Ministers to member states on "special investigative techniques" in relation to serious crimes including acts of terrorism* (20 April 2005), Rec(2005)10, Chapter II (a) (available at https://wcd.coe.int/ViewDoc.jsp?id=849269&Site=CM; accessed 2 February 2012).
11. Ibid., Chapter II (b) (4).
12. Ibid., Chapter II (b) (5).
13. Ibid., Chapter II (b) (6).
14. Germany, Act Restricting the Privacy of Correspondence, Posts and Telecommunications (June 26, 2001), *Federal Law Gazette I*, p. 1254, revised 2298, last amended by Article 1 of the Act of July 31, 2009, *Federal Law Gazette I*, p. 2499, Section 3 (2).
15. For a fuller discussion of this point, see Gregory Rose and Diana Nestorovska, "Terrorism and National Security Intelligence Laws: Assessing Australian Reforms" in *LAWASIA Journal* (2005), pp. 127–155.
16. Council of Europe, European Commission for Democracy through Law (Venice Commission), *Report on the democratic oversight of the security services*, CDL-AD(2007)016 (2007), pp. 44–45 (available at http://www.venice.coe.int/docs/2007/CDL-AD%282007%29016-e.asp; accessed 22 October 2011).
17. Canadian Security Intelligence Service Act (31 August 2004), R.S.C., 1985, Chapter C-23, Section 21 (2) (available at http://www.csis-scrs.gc.ca/pblctns/ct/cssct-eng.asp).
18. Argentina, National Intelligence Law, Law 25520 of 2001, Title VI, Article 18.
19. Federal Judicial Center web site, "Foreign Intelligence Surveillance Court" (available at http://www.fjc.gov/history/home.nsf/page/courts_special_fisc.html).
20. South Africa, Regulation of Interception of Communications and Provision of Communication-Related Information Act, Act No. 70 of 2002, *Government Gazette*, Vol. 451, No. 24286 (22 January 2003), Section 24 (available at www.info.gov.za/gazette/acts/2002/a70-02.pdf; accessed 2 February 2012).
21. Argentina, National Intelligence Law, Law 25520 of 2001, Title VI, Article 34II.
22. Germany, Act Restricting the Privacy of Correspondence, Posts and Telecommunications (June 26, 2001), *Federal Law Gazette* I, p. 1254,

revised 2298, last amended by Article 1 of the Act of July 31, 2009, *Federal Law Gazette I*, p. 2499, Section 14.

23. Ibid., Section 5.
24. L. Britt Snyder, *Sharing Secrets with Lawmakers: Congress as a User of Intelligence* (Washington: Central Intelligence Agency, February 1997) p. 49 (available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sharing-secrets-with-lawmakers-congress-as-a-user-of-intelligence/toc.htm; accessed 14 February 2012).
25. Imtiaz Fazel, "Who shall guard the guards? Civilian oversight and the Inspector General of Intelligence," in *To spy or not to spy? Intelligence and democracy in South Africa*, ed. Lauren Hutton (Pretoria: Institute for Security Studies, 2009), pp. 35–36.
26. Belgium, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18 July 1991); See also the Belgian Standing Intelligence Agencies Review Committee web site (available at www.comiteri.be).
27. Belgium, Loi relative aux méthodes de recueil des données par les services de renseignement et de sécurité (4 février 2010).
28. Belgium, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18 July 1991), Article 34.
29. Ibid., Section 15.
30. Germany, Act Restricting the Privacy of Correspondence, Posts and Telecommunications (G10 Act), (June 26, 2001), *Federal Law Gazette I*, p. 1254, revised 2298, last amended by Article 1 of the Act of July 31, 2009, *Federal Law Gazette I*, p. 2499, Section 15.

TOOL 6

Overseeing the Use of Personal Data

Ian Leigh

SIX

6

Overseeing the Use of Personal Data

Ian Leigh

1. INTRODUCTION

This tool looks at how oversight bodies can ensure that intelligence services use personal data in compliance with the law governing the services. It aims to explain the role that oversight bodies play in examining how intelligence services store, access, and transfer personal data. It does not address the collection of personal data by intelligence services (covered in Hutton—Tool 5) or the sharing of personal data with domestic and foreign partners (covered in Roach—Tool 7).

The topics this tool considers include: risks arising from the use of personal data by intelligence services, appropriate legal frameworks for regulating such usage, and the means to oversee such usage. It concludes with a brief summary of key principles for enacting legislation on the use of personal data by intelligence services.

In accordance with widespread international legal practice, this tool will use the term *personal data* to mean "any information relating to an identified or identifiable individual ('data subject')."[1]

2. RISKS OF PERSONAL DATA USAGE BY INTELLIGENCE SERVICES

Intelligence services have legitimate reasons relating to their legal mandates to collect, store, process, and disclose personal data. The individuals to which the data relates may be legitimate targets of interest because of suspected involvement in espionage or terrorism, for example. The need to collect such information will vary from country to country and service to service according to the service's precise legal responsibilities.

There is, however, a constant danger of overbroad collection of personal data. The process of establishing, for instance, whether a suspect person is engaged in terrorist activities contemplates the possibility that the information collected will lead to a negative conclusion. Plainly, in such a situation, the initial collection of information cannot be called improper; but once the service has established that the individual is not involved, it should not continue to collect information (or, arguably, even retain and use the information it has collected). Doing so, moreover, runs the risk that the service will be tempted to collect information in increasingly widening circles—for example, collecting information on associates of the suspect or the civil society organization to which they belong. This can have a chilling effect, leading individuals to become fearful of participating in such lawful civil society organizations as trade unions, separatist political parties, and environmental or anti-nuclear groups. There also exists the more general danger that personal data stored in the files of an intelligence service may be misused—by officials in transitional states, for example, in order to blackmail political opponents or stifle journalists.

It is sometimes argued that that the mere storage, classification, analysis, and retention of information by intelligence services is benign. While the collection of personal data poses more obvious threats (see Hutton—Tool 5), its storage is potentially harmful because personal data is closely linked to personal autonomy. The control that individuals have over their own lives—in particular, the choices they make with regard to personal details (to whom, to what extent, and for what purpose they choose to disclose them)—is eroded when government agencies are permitted to assemble personal data from multiple sources.

In amassing personal information on individuals, intelligence services acquire a measure of control over the subjects of that information. In the worst cases, personal data held by services may be used improperly to exert pressure on politicians or journalists. Even the knowledge that the services hold personal data can be psychologically disturbing for the individuals concerned, even if no harmful disclosure ever takes place. Similarly, participation in civil society may be stunted by the knowledge (or undispelled suspicion) that information about certain forms of political, industrial, and social activism is being retained in security files.

Bearing in mind the oft-stated need to retain security information for long periods of time, the prospect of harm may affect individuals for many years or decades. Information relating to a person's youthful activities, for example, may in some cases be retained into that person's old age, even if his or her later life gives no reason for him or her to be treated as a security risk.

Furthermore, personal data held by intelligence services may be partial, inaccurate, or out

of date. In extreme instances, it may even have been obtained from sources with a desire to harm the person concerned out of personal animosity or jealousy. Similarly, sources motivated by monetary reward may have an incentive to exaggerate or embroider facts when supplying information about people.

Other risks relating to the storage of personal data include the unprecedented capacity of some intelligence services to link, through privileged access, information about an individual contained in otherwise separate law enforcement, medical, and tax-related databases.

The risks, of course, do not end with the storage, classification, and analysis of personal data. There are also risks associated with its use. Some uses are legitimate (such as security vetting), while others are less creditable (such as racial or religious profiling or the exertion of a hidden influence on a person). An unattributed disclosure of personal data to the media, for example, can cause the individual to whom the information relates harm and loss of opportunity. His or her professional standing may be affected, such as through the denial or loss of a security clearance; and, more generally, his or her reputation may be damaged. Similarly, the disclosure of unsubstantiated or inaccurate data to foreign governments may result in the denial of travel opportunities or worse (see Roach–Tool 7).

Intelligence services have a strong interest in assuring that the information they hold on legitimate targets is fair, accurate, and up-to-date. The service's effectiveness and reputation may be adversely affected if it discloses, gives advice on, or acts on wrong, incomplete, or out-of-date information. Nevertheless, there are certain risks inherent to intelligence work that strengthen the case for external control and oversight of information-handling procedures. In particular, the pressure services feel to anticipate future security risks can encourage overbroad collection of information on an ever-increasing number of individuals. Technological changes, such as improvements in data mining, can likewise encourage the collection and storage of vast quantities of personal information—such as data on e-mail traffic, web searches, airline reservations, and financial transactions.

3. LEGAL FRAMEWORK FOR USE OF PERSONAL DATA BY INTELLIGENCE SERVICES

The right to privacy is protected under human rights law as established by the major international treaties.[2] For reasons of relevance and practicality, however, this tool will concentrate on the human rights standards applicable within Europe, especially those set forth in the European Convention on Human Rights (ECHR), which are the most developed. Although this tool focuses on the right to privacy, the collection and use of personal data by intelligence agencies may also impact indirectly other human rights, such as the rights to free expression and free association.

Article 8 of the ECHR, which applies to the forty-seven member states of the Council of Europe, states:

> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> [The European Court of Human Rights (ECtHR) has interpreted this provision to include telephone calls and other means of electronic communication.]

> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

The Charter of Fundamental Rights of the European Union is also significant in that it contains explicit provisions for the protection of personal data that are binding on the member states of the European Union (EU). Article 8 states:

> *1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
>
> *3. Compliance with these rules shall be subject to control by an independent authority.*

Furthermore, according to Article 52.1 of the Charter:

> *Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*

However, because these provisions of the Charter of Fundamental Rights have yet to give rise to any jurisprudence, this tool will focus primarily on the ECHR.

The ECtHR has found that government security files containing personal data are clearly within the protected scope of private life enunciated in Article 8 of the ECHR. The court has also found in several cases that the collection, storage, and release of personal data by an intelligence service constitutes an "interference" with the right to respect for private life—permissible only under the strict criteria set forth in Article 8.2. The court's findings apply not only to the disclosure of information to other government agencies but also to its use for internal vetting and security clearance.[3] In deciding the case of Rotaru v. Romania (2000), which concerned security files held by the Romanian intelligence services, the court found that:

> *both the storing by a public authority of information relating to an individual's private life and the use of it and the refusal to allow an opportunity for it to be refuted amount to interference with the right to respect for private life secured in Article 8.1 of the Convention.*[4]

3.1 PERMISSIBLE LIMITATIONS ON THE RIGHT TO PRIVACY

In order for an intelligence service's storage and use of personal data to be compatible with the ECHR, it must satisfy the criteria set forth in Article 8.2. That is, the use must be "in accordance with the law," "necessary in a democratic society," and "in the interests of national security."

The test for "in accordance with law" imposes a stringent criterion. If that criterion cannot be met, there will be a violation of Article 8 regardless of the broader interests at stake.

Thus, the legality requirement prods parliamentarians to establish a sound statutory basis for the use of personal data by intelligence services.

The ECtHR has interpreted "in accordance with the law" to mean that any restriction of the right to privacy should have "some basis in domestic law" and that it meet the test of "quality of law," which the court defined as being "accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and [being] compatible with the rule of law."[5]

Applying these tests, the ECtHR has found breaches of Article 8 where no law exists to govern intelligence services or where such a law exists but it fails to include provisions regulating the collection and storage of personal data.[6] Furthermore, under the "quality of law" test, such a law "must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which [the law can be used]."[7] In addition, because "implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large," laws governing the collection of personal data must not allow "the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power" and consequently must "indicate the scope of any such discretion conferred…and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."[8]

In considering such laws, the court checks that they specify sufficiently clearly, inter alia, the procedures to be followed for examining, using, and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings obtained by surveillance can or must be destroyed.[9]

A recent case involving the Russian government illustrates these principles.[10] The court found that the registration of a human rights activist in a secret surveillance database violated Article 8 of the ECHR. Because the database was created on the basis of an unpublished ministerial order that was not accessible to the public, members of the public could not know why certain individuals were registered in the database, what type of information was being stored, how it was being stored, for how long it would be stored, how it would be used, and who would have control over it.

The "quality of law" test does take into account, however, legitimate security concerns. In the context of security vetting, for example, the "foreseeability" portion of the test does not require that applicants be able to predict the process entirely (or else it would be easy to circumvent). Rather, the authorizing law needs only to give a general description of the practice.[11]

Box 1: The "quality of law" test in practice

In *Rotaru v. Romania*[12] the European Court of Human Rights examined a Romanian law on the regulation of security files kept by the government. The court held that the law was insufficiently clear in describing the circumstances in which it could be used—specifically, the uses to which the personal information in the files could be put—nor did the law establish any mechanism for monitoring the use of the information.

The Court also found the law defective because it did not "indicate" with reasonable clarity the scope of the discretion being conferred on the Romanian government. That is, the law failed to limit exercise of the government's powers to gather, record, and archive personal information in secret files. In particular, the law did not define the kind of information that could be recorded, the categories of people against whom surveillance measures could be taken, the circumstances in which such measures could be taken, and the procedures to be followed. Nor did it include any limitations on the length of time for which it could be held.[13]

With regard to security archives kept by prerevolutionary intelligence services, the law permitted these archives to be consulted but failed to include "explicit, detailed provisions concerning the persons authorised to consult the files, the nature of the files, the procedure to be followed or the use that may be made of the information thus obtained."[14]

Once the clarity, accessibility, and foreseeability hurdles of the "quality of law" test are passed, the ECHR requires an examination of the purpose and necessity of the interference with private life. This entails an evaluation of proportionality—that is, whether the interference is excessive, even if one takes into account the legitimate aim of protecting national security. For example, in a recent case, the ECtHR found that the Swedish government had violated Article 8 of the ECHR when it retained personal data in a security file for a period exceeding thirty years. In view of the nature and age of the information, the court did not accept the defence that the decision to continue storing the information was supported by relevant and sufficient reasons of national security.[15]

In considering whether an interference with private life is "necessary in a democratic society," the court takes into account what safeguards have been created to oversee the storage and use of personal data—especially those involving independent bodies.[16] Where no safeguards exist to allow a person to protect his or her right to a private life, the court will find a violation of Article 8. In *Turek v. Slovakia* (2006), for instance—a case in which the applicant complained about being registered as a collaborator with the former Czechoslovak Communist security agency, the issuing of a security clearance to that effect, and the dismissal of his action challenging that registration—the court found that the absence of a procedure by which the applicant could seek protection of his right to a private life violated Article 8.[17]

Even when such a procedure exists in law, excessive delays in responding to requests by members of the public for access to their information can be considered a violation (because the safeguards are not effective). For example, in *Haralambie v. Romania* (2009), the court found the Romanian government's delay of six years in allowing access by the applicant to his personal security file, created under the previous Communist regime, violated his rights under Article 8 of the ECHR.[18]

The need therefore exists for clear legal limits to be placed on the collection and use of personal data by intelligence services and for oversight bodies to ensure that the services comply with laws regulating the management of such data. The UN special rapporteur on

the promotion and protection of human rights and fundamental freedoms while countering terrorism reiterated this need in his 2010 report to the UN Human Rights Council:

> *Publicly available law outlines the types of personal data that intelligence services may hold, and which criteria apply to the use, retention, deletion and disclosure of these data. Intelligence services are permitted to retain personal data that are strictly necessary for the purposes of fulfilling their mandate.*[19]

3.2 DATA PROTECTION PRINCIPLES

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[20] ("the Data Protection Convention") lays down minimum principles for member states in the field of data protection (see Table 1). Under the Data Protection Convention, each signatory state commits to "take the necessary measures in its domestic law to give effect to the basic principles for data protection"[21] and to "establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection."[22] In addition, aspects of these principles—especially those that relate to fair processing, consent, lawful authority, subject access, and rectification—can be found in Article 8.2 of the Charter of Fundamental Rights of the European Union.

TABLE 1: COUNCIL OF EUROPE DATA PROTECTION PRINCIPLES

Data protection principle	Requirements
Quality of data (Article 5)	Personal data undergoing automatic processing shall be: a. obtained and processed fairly and lawfully; b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes; c. adequate, relevant and not excessive in relation to the purposes for which they are stored; d. accurate and, where necessary, kept up to date; e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.
Data security (Article 7)	Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.
Right to establish the existence of personal data (Article 8)	Any person shall be enabled: to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file.
Right to access (Article 8)	Any person shall be enabled: ▪ to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form. ▪ to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention.
Right to have a remedy (Article 8)	Any person shall be enabled: to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

The Data Protection Convention (in Article 11) states that the principles contained therein are meant to be minimum standards, capable of being supplemented with wider measures of protection.

The manner in which the Data Protection Convention addresses restrictions on the data protection principles is similar to that in which the ECHR addresses restrictions on the right to privacy (discussed above). Restrictions must be "provided for by the law [of the signatory state]" and must constitute "a necessary measure in a democratic society"[23] for the protection of a legitimate interest, such as national security or the rights of the data subject.[24]

3.3 RELEVANCE OF NATIONAL LEGISLATION

Because potentially serious damage to human rights can arise from the collection, handling, and disclosure of personal data by intelligence services, it is appropriate that guidelines for the management and use of such data be democratically enacted in publicly accessible legislation. This practice has several advantages: it encourages reflective political debate on the proper scope of intelligence service activity, it removes decision making from service or executive discretion, and it gives the services a clear mandate with regard to actions that may infringe on human rights.

Legislation governing the use of personal data by intelligence services may address one or more of the following topics:

- permissible and impermissible reasons for processing personal data
- limits on the disclosure of personal data
- public disclosure of the types of data being stored
- access to personal data by the data subject
- notification that personal data has been collected
- review, revision, and erasure of personal data

3.3.1 Permissible and impermissible reasons for processing personal data

Legislation of this kind may specify the types of personal data that can be collected and retained as well as when a file containing personal data can be opened (see Box 2). Recognizing explicitly the principle of proportionality, German law relates the need to collect data to the seriousness of the corresponding threat. Specifically, it requires Germany's domestic intelligence service (the Federal Office for the Protection of the Constitution) to consider whether the desired information can be obtained from open sources or using means that infringe less on the right to privacy.[25] Such legislation may also reduce the likelihood that intelligence services violate human rights by prohibiting certain forms of conduct, such as the targeting of individuals based on racial or religious characteristics or their political views.

Box 2: Limits on the processing of personal data in selected jurisdictions

This box contains provisions from Dutch and Argentine law that limit the processing of personal data by intelligence services on the grounds of impermissible criteria.

The Netherlands[26]

"The General Intelligence and Security Service may only process personal data relating to persons:

a. who give cause to serious suspicion for being a danger to the democratic legal system, or to the security or other vital interests of the state;
b. who have given permission for a security clearance investigation;
c. for whom this is necessary within the context of the investigations regarding other countries;
d. about whom information has been obtained by another intelligence or security service;
e. whose data are necessary to support a proper performance of the service's duties;
f. who are currently or have been employed by a service;
g. concerning whom this is necessary within the context of drawing up threat and risk analyses as referred to in Article 6, second paragraph, under e."

Argentina[27]

"No intelligence agency shall…keep data on individuals because of their race, religion, private actions, and political ideology, or due to their membership in partisan, social, union, community, co-operative, assistance, cultural or labour organisations, or because of legal activities performed within any field."

3.3.2 Limits on the disclosure of personal data

Legal limits on the disclosure of personal data are generally desirable, especially to prevent the leaking of information for partisan political reasons. Restrictions of this sort are particularly important in transition states, where the delicate task of building trust in the neutrality of security institutions can be severely undermined by partisan conduct. Many countries impose criminal liability on intelligence officers who disclose information in their service's files, including personal data, without lawful authority or for unauthorized purposes (see Box 3).

Box 3: Prohibiting improper disclosure of personal data in Romania

This provision from Romanian law illustrates how personal data can be protected from improper disclosure by intelligence officers:

> "The information regarding the private life, the honor or reputation of the persons, incidentally known on the occasion of the getting the data necessary to the national security, may not be made public. The disclosure or the utilisation, outside the legal framework, by employees of the intelligence services, of information, of the data provided under paragraph 1, shall be considered an offence and should be punished with imprisonment from 2 to 7 years."[28]

3.3.3 Public disclosure of the types of data being stored

Data protection legislation in some countries requires state agencies such as intelligence services to publish details of the types of personal data that they hold, the purposes for

which the data was collected, the purposes for which it may be disclosed, descriptions of the databases in which it is kept, and the conditions and controls applicable to these databases. Publication of this information helps to strengthen both transparency and accountability. Individuals who wish to exercise their rights of subject access and rectification can learn from this information which state agencies hold their personal data, as well as the scope of and reasons for such holdings.

In principle, imposing a duty on intelligence services to disclose their holdings of personal data is desirable because it helps to strengthen the agencies' legitimacy and allay inaccurate speculation about their work. This disclosure is beneficial even when there is good reason on national security grounds to prevent an individual from discovering whether personal data on him or her is being held by an intelligence service—for example, where a "neither confirm nor deny" response to a request for subject access would be justified.

Box 4: The duty to disclose information concerning databanks under Canadian law

This provision from Canadian law illustrates a general duty to publish information about personal information databases:

> "The head of a government institution shall cause to be included in personal information banks all personal information under the control of the government institution that (a) has been used, is being used or is available for use for an administrative purpose; or (b) is organized or intended to be retrieved by the name of an individual or by an identifying number, symbol or other particular assigned to an individual."[29]

3.3.4 Access to personal data by the data subject

Many countries have enacted data protection or privacy laws that recognize the right of data subjects to access personal data about themselves held by government agencies (see Box 5). Some data protection laws additionally recognize the subject's right to rectify the information, to have a statement included with the information disputing its accuracy, or to have the information destroyed. For reasons of national security, such laws invariably include special provisions for data held by intelligence services. These provisions take a variety of forms.

In some countries, services are granted *exemption* from data protection laws, which simply do not apply to information that they hold. In such cases, there exists no right of subject access. This approach has the advantage of simplicity, but it can be seen as overbroad because exemptions relieve the services of any obligation to explain how national security concerns justify the withholding of particular data. This approach may also prevent the operation of normal external oversight and controls—limiting the jurisdiction, for instance, of a privacy commissioner.

A variation on this approach is to exempt intelligence services from freedom of information legislation only. In such cases, data protection laws (including the right of subject access) continue to apply, at least in principle, although in practice subject to review on a case-by-case basis.

Box 5: The right of access to personal data held by intelligence services under Dutch law

These provisions from Dutch law illustrate a qualified right of subject access to personal data held by intelligence services:[30]

"Article 47
1. The relevant Minister will inform anyone at his request as soon as possible but at the latest within three months whether, and if so which, personal data relating to this person have been processed by or on behalf of a service."

"Article 48
1. The person who pursuant to Article 47 has inspected processed information concerning him by or on behalf of a service may submit a written statement with respect to this. This statement will be added to the relevant information."

"Article 53
1. A request as referred to in Article 47 will in any case be dismissed if:
   a. within the context of any investigation information has been processed concerning the person making the request, unless:
      i. the relevant information was processed more than 5 years ago,
      ii. since then with regard to the person making the request no new information has been processed in connection with the investigation pertaining to which the relevant information has been processed, and is information is not relevant to any current investigation;
   b. no information has been processed with regard to the person making the request."

Other countries instead include in their data protection legislation *exceptions* based on national security. These are narrower and more specific than exemptions, because they place upon the intelligence service the burden to justify on a case-by-case basis why an individual's rights under the data protection laws should not apply.

Such legislation may grant individuals a prima facie right of subject access, exercised simply by applying to an executive oversight body but also subject to restrictions designed to safeguard ongoing investigations and protect sources and methods.[31] (All such restrictions should be in accordance with governing law, proportionate to the threat, and subject to independent review.[32]) Quite apart from the human rights at stake, such an approach can act as a safeguard against mismanagement and corruption.

Commonly, exceptions of this kind allow a service to issue a "neither confirm nor deny" response in order to deter speculative and potentially threatening applications intended to establish the extent of a service's information holdings.

In practice, the application of exceptions may result in the refusal of most requests. Thus, the outcome of the exception approach may not seem very different than the outcome of the exemption approach. There is an important distinction, however: the exception approach requires the agency to justify non-disclosure against a legal presumption favouring disclosure, while the exemption approach does not. Additionally, the claim of an exception is reviewable by an independent authority in a way that the claim of an exemption is not. Empirical research on the operation of the Canadian Access to

Information Act of 1982 and the Canadian Privacy Act of 1982 confirms the benefits of subjecting the information-handling processes of intelligence services to outside scrutiny by an independent body—not least in stimulating internal awareness of information and privacy concerns.[33]

A further variation is to designate only certain databanks as "exempt," thereby making them in principle subject to different oversight mechanisms but in practice relieving the intelligence service of the duty to respond in detail to individual requests. Canada uses this model as a complement to the exceptions approach.

Alternatively, governing law may empower a minister, subject to review, to issue a blanket certificate of exemption (such as under the UK Data Protection Act[34]). Doing so conveys a high measure of assurance to intelligence services that their files will not be disclosed in a manner that, for instance, contradicts undertakings given to allies and informants. On the other hand, such certificates are typically overbroad, removing external scrutiny and the benefits that it brings, including public confidence in service propriety. Justifiable concerns regarding information security are better met with specific exceptions than blanket exemptions. Moreover, beyond subject access and rectification, the data protection principles relating to quality of data and data security are also of obvious relevance to intelligence services and therefore provide further reason for not exempting services from the jurisdiction of data protection laws.

Box 6: Access to personal data held by intelligence services: good practice identified by the UN special rapporteur

"Individuals have the possibility to request access to their personal data held by intelligence services. Individuals may exercise this right by addressing a request to a relevant authority or through an independent data-protection or oversight institution. Individuals have the right to rectify inaccuracies in their personal data. Any exceptions to these general rules are prescribed by law and strictly limited, proportionate and necessary for the fulfilment of the mandate of the intelligence service. It is incumbent upon the intelligence service to justify, to an independent oversight institution, any decision not to release personal information."[35]

3.3.5 Notification that personal data has been collected

Some countries (such as the Netherlands[36] and Germany[37]) require that the subjects of personal data collection (especially by surveillance) be notified ex post facto and subject to certain limits that information has been collected about them (see Box 7). In theory, this practice allows for the possibility of retrospective challenge and places a check upon the intelligence service decision to open a file on the subject. However, restrictions placed on the right to notification in order to protect ongoing operations and the identities of sources may render the right illusionary in many cases. For this reason, the practice is currently under review in the Netherlands.[38]

Alternatively, where there is no right of notification or rectification, the risks of personal data usage by intelligence services are bound to be exacerbated, and the need for other controls is correspondingly greater.

Box 7: The duty to notify data subjects under German law

These provisions from German law illustrate the principle of notification:

"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."[39]

"Where the collection of data in accordance with subsections 2 and 1 is concerned, the nature and importance of which is tantamount to a restriction of letter, postal and telecommunications privacy, in particular comprising eavesdropping on and recording of private conversations with clandestine technical means,

1. the data subject shall be informed of the measure after its termination, as soon as it can be ruled out that the purpose of the measure is jeopardised, and
2. the Parliamentary Control Panel shall be notified."[40]

3.3.6 Review, revision, and erasure of personal data

Another way in which the data protection principles can be implemented is to impose a duty on the intelligence services to review periodically whether their personal data files are accurate, up-to-date, and relevant to their mandate.[41] In some countries this duty is associated with supplementary duties to correct or destroy information that is incorrect[42] or no longer relevant.[43]

If only so that their reports can be based on accurate information, intelligence services need to establish procedures for reviewing and revising personal data to make sure that it is up-to-date and complete (insofar as it is relevant to the services' lawful activities). Out-of-date information can be misleading and therefore more dangerous even than ignorance. Furthermore, from the point of view of the data subject, personal information that is correct and up-to-date is much less likely to result in an injustice, such as the denial of a security clearance or an adverse immigration decision.

Box 8: Regular assessments of data held by intelligence services: good practice identified by the UN special rapporteur

"Intelligence services conduct regular assessments of the relevance and accuracy of the personal data that they hold. They are legally required to delete or update any information that is assessed to be inaccurate or no longer relevant to their mandate, the work of oversight institutions or possible legal proceedings."[44]

Because of the preventative and anticipatory nature of threat assessment by the intelligence services, some individuals may legitimately come to the attention of the services before additional information is collected that establishes they are not proper targets for further data collection. A subject, for example, may be found to be an associate

of a legitimate target but not a conspirator herself/himself; or the subject may simply have a name similar to the name of a legitimate target. Requiring an intelligence service to close its file on such a subject can prevent possible abuse.

Similarly, tangential information on individuals collected during an operation that has run its course should be erased. The German law governing the activities of the Federal Office for the Protection of the Constitution contains several provisions relevant to this concern. It stipulates, for example, that the collection of information must cease "as soon as its purpose has been achieved or if there are indications that it cannot be achieved at all or by employing these assets."[45] The law also imposes duties to review (every five years) previously collected data, to correct inaccurate data (with inaccurate or contested data noted as such in the relevant files[46]), and to erase data that is no longer required (see Box 9). Beyond protecting data subjects, these duties assist in the task of oversight.

Box 9: The duties to review, correct, and erase personal data under German law

These provisions from German law illustrate the principles of review, revision, and erasure: "(1) Incorrect personal data stored in files shall be corrected by the Federal Office for the Protection of the Constitution.

(2) 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.

(3) 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."[47]

4. THE ROLE OF OVERSIGHT BODIES

This section discusses the ways in which oversight bodies can monitor the use of personal data by intelligence services to ensure that the data is not misused. Although the section focuses primarily on external oversight, the importance of internal mechanisms should not be overlooked. These include specific procedures for determining when files should be opened or closed, which officers should have access to them, when their contents should be reviewed, and how they will be kept secure.

Effective external oversight, on the other hand, depends on the existence of independent bodies with adequate legal powers and resources to fulfil their mandates (see Table 2). The UN special rapporteur has emphasized the need for an independent institution that "has access to all files held by the intelligence services and has the power to order the disclosure of information to individuals concerned, as well as the destruction of files or personal information."[48] The Charter of Fundamental Rights of the European Union makes compliance with data protection rules "subject to control by an independent authority."[49] At the national level, Swedish law guarantees the autonomy and resources of the Swedish Commission on Security and Integrity Protection,[50] while Hungarian law imposes a specific

duty on the intelligence services to cooperate with independent oversight bodies regarding the services' use of personal data.[51]

TABLE 2: CHARACTERISTICS OF INDEPENDENT EXTERNAL OVERSIGHT BODIES

Institution	Independence	Remit	Methods	Outcomes
Ombuds institution	Autonomous	Individual complaints	Investigation	Recommendation
Data protection commissioner	Autonomous	Compliance with data protection laws	Investigation, sampling	Report, directive
Tribunal	Autonomous	Individual complaints	Adversarial process	Binding decision
Parliamentary committee	Partisan	Referrals, own-initiative reporting	Parliamentary hearings	Report

In transitional and postconflict states, newly democratized services often take custody of large archives of security files containing information collected by the previous regime. The management of these files can create unusual challenges, particularly when (for sound democratic reasons) the country's security and intelligence sector has been drastically reduced in size. In these situations, independent oversight bodies can play a helpful role in auditing file-management practices through various means.

In general, the functions of independent oversight bodies with regard to personal data are governed in part by standards set forth in human rights law. With regard to post hoc remedies, for example, Article 13 of the ECHR requires that "Everyone whose rights and freedoms…are violated shall have an effective remedy before a national authority." With its decision in *Segerstedt-Wiberg v. Sweden* (2006), the ECtHR found that, although the Article 13 test is generally subsidiary to the Article 8 tests of "in accordance with the law" and "necessity in a democratic society," the absence of a remedy provision in national legislation may result in a violation of the convention. Elsewhere, the court has held that, even in the context of national security, the remedy procedure required by Article 13 must be effective *in practice* as well as in law.[52]

In *Association for European Integration and Human Rights v. Bulgaria*, an interception of communications case alleging violation of both Article 8 and Article 13, the Court referred approvingly to several examples of independent remedies that satisfy the Convention's requirements. These included: the right of complaint to an expert oversight body (the G10 Commission) and to the Constitutional Court in Germany, the right of appeal to the Council of State in Luxembourg, the right of recourse to a special tribunal in the UK, and the right of complaint to an expert oversight body in Norway.[53] (For a detailed discussion of complaint handling, see Forcese—Tool 9).

With respect to the use of personal data by intelligence services, the key issues of oversight mirror those of legal standards—namely, collection of data, storage of data, subject access, notification, review, rectification, and erasure. Because the scope of these issues is broad, the jurisdiction of oversight bodies must be equally broad. The authority of the German G10 Commission, for example, extends "to the entire scope of collection, processing and use of the personal data obtained pursuant to this Act by intelligence

services of the Federation, including the decision on notification of data subjects."[54]

Oversight of this kind is necessary to ensure that services comply with the personal data standards discussed above. Bearing in mind the secretive nature of intelligence work, such oversight is more likely to be effective and command public respect if it is continuous (or at least periodic), rather than simply reactive to public complaints or allegations of abuse. A number of countries, therefore, have made provisions for ongoing scrutiny in the mandates of independent bodies responsible for the oversight of intelligence services. In Norway, for example, the Parliamentary Intelligence Oversight Committee (an expert oversight body) has a legal duty to conduct six inspections of the Norwegian Police Security Service each year. These inspections must include at least ten random archival checks and, at least twice yearly, a review of all current surveillance cases.[55] Denmark's Control Committee on Police and Military Intelligence Services (Wamberg Committee)—named after its first chair, A. M. Wamberg—plays a similar role (see Box 10).

Box 10: Denmark's Control Committee on Police and Military Intelligence Services (Wamberg Committee)

The primary task of the Wamberg Committee is to supervise the registration and dissemination of personal data by the Danish Security and Intelligence Service (PET). When a person or organization becomes the subject of an intelligence investigation, PET may wish to register a file on that person or organization. Such files are subject to review by the Wamberg Committee, which must approve the registration of new files on Danes and on foreign nationals residing in Denmark.

The committee consists of a chair and three other members. All are appointed because of the general confidence and respect they enjoy. Each must also be considered apolitical.

The committee meets six to ten times a year at the PET offices to review cases and decide whether the criteria for registering them have been met. At the same time, the committee randomly samples old files to establish whether the deadlines for deletion are being met. The committee also discusses the principles of registration regularly with the Ministry of Justice.

In a number of countries, an individual with a complaint about the way an intelligence service has handled his or her personal data can be heard by an independent body with the power to inspect the service's files and determine for itself whether data has been misused (see Forcese–Tool 9). Under Swedish law, for example, the Commission on Security and Integrity Protection has the authority, when responding to a complaint, to review the legality of security service activities relating to the use of personal data (see Box 11). The Commission also has the authority to review the release of personal data from various police and security registers in order to ensure that the release complies with Swedish statutory and constitutional law, including human rights standards and the principle of proportionality.[56]

Box 11: Sweden's Commission on Security and Integrity Protection

These provisions from Swedish law describe the responsibilities of the Commission on Security and Integrity Protection (an expert oversight body):

"1. The Commission on Security and Integrity Protection (the Commission) shall supervise the use by crime-fighting agencies of secret surveillance and qualified assumed identities and associated activities.

The Commission shall also supervise the processing of data by the Swedish Security Service under the Police Data Protection Act, particularly with regard to Section 5 of that Act.

The supervision shall aim in particular at ensuring that activities under the first and second paragraphs are conducted in accordance with laws and other regulations.

2.The Commission shall exercise its supervision through inspections and other investigations.

The Commission may make statements on established circumstances and express its opinion on the need for changes in the activities and shall strive to ensure that any deficiencies in laws and other regulations are remedied.

3. At the request of an individual, the Commission is obliged to check whether he or she has been the subject of secret surveillance or subject to processing of personal data as defined in Section 1 and whether the use of secret surveillance and associated activities or the processing of personal data was in accordance with laws and other regulations. The Commission shall notify the individual that the check has been carried out."[57]

5. RECOMMENDATIONS

This section recommends principles that parliamentarians, in particular, can follow in establishing an appropriate legal framework for the use of personal data by intelligence services in a manner consistent with human rights obligations.

- The legislative mandate of each intelligence service should specify the purposes for which personal data can be lawfully gathered and files lawfully opened.
- The law governing the intelligence services should establish effective controls on how personal data is used and for how long it may be retained. These controls should comply with internationally accepted data protection principles. Such law should also require checks, carried out by independent personnel (that is, overseers external to the intelligence community), in order to ensure that the controls are indeed effective.
- The law governing the intelligence services should not exempt intelligence services from domestic privacy and data protection laws. Instead, the services should be permitted, when relevant to their mandate, to take advantage of exceptions to disclosure regulations based on a limited concept of national security.
- Whether such exceptions have been applied correctly should be determined by an independent oversight body with appropriate access to relevant data in the service's files.

- Individuals complaining that the storage, use, or disclosure of their personal data by an intelligence service has violated their privacy should have the right to an effective remedy before an independent body.
- The decisions of intelligence services to store personal data should be reviewed by an independent oversight body, as should requests for subject access and decisions to retain, transfer, and delete personal data.

Endnotes

1. This definition appears in Article 2(a) of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and Section 1(b) of the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. A similar definition appears in Article 2(a) of European Union Directive 95/46/EC; however that directive does not apply to state security activities (see Article 3.2).
2. Article 17 of the International Covenant on Civil and Political Rights states that "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks." Article 12 of the Universal Declaration of Human Rights states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."
3. *Leander v. Sweden*, No. 9248/81, European Court of Human Rights (ECHR), 1987.
4. *Rotaru v. Romania*, No. 28341/95, ECHR, 2000, Paragraph 46.
5. *Weber and Saravia v. Germany*, No. 54934/00, ECHR, 2006, Paragraph 84.
6. R. V. v. *The Netherlands*, No. 14084/88, ECHR, 1991.
7. *Weber and Saravia v. Germany*, No. 54934/00, ECHR, 2006, Paragraph 93.
8. Ibid., Paragraph 94.
9. See, for example, the detailed analysis of the German G10 law in *Weber and Saravia v. Germany*, admissibility decision, No. 54934/00, ECHR, 2006.
10. *Shimovolos v. Russia*, No. 30194/09, ECHR, 2011.
11. *Leander v. Sweden*, No. 9248/81, ECHR, 1987.
12. *Rotaru v. Romania*, No. 28341/95, ECHR, 2000.
13. Ibid., Paragraph 57.
14. Ibid.
15. *Segerstedt-Wiberg and Others v. Sweden*, No. 62332/00, ECHR, 2006.
16. *Leander v. Sweden*, No. 9248/81, ECHR, 1987, Paragraphs 52–57; see also *Rotaru v. Romania*, No. 28341/95, ECHR, 2000, Paragraph 59.
17. *Turek v. Slovakia*, No. 57986/00, ECHR, 2006.
18. *Haralambie v. Romania*, No. 21737/03, ECHR, 2009.
19. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: 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*, United Nations Document A/HRC/14/46 (17 May 2010), p. 21 (Practice 23).
20. Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108 (Strasbourg, 28.I.1981). The Convention builds on the widely influential OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980) (available at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#part2).The OECD Guidelines established eight basic data protection principles concerning collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.
21. Ibid., Article 4.
22. Ibid., Article 10.
23. The term *necessary measure* is to be understood within the context of the doctrine of proportionality enunciated in the Charter of Fundamental Rights of the European Union.
24. Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108 (Strasbourg, 28.I.1981), Article 9.
25. Germany, Federal Act on Protection of the Constitution (20 December 1990), *Federal Law Gazette I*, p. 2954, 2970, last amended by Article 1a of the Act of 31 July 2009, *Federal Law Gazette I*, p. 2499, 2502, Section 9.
26. The Netherlands, Intelligence and Security Services Act 2002, Article 13.
27. Argentina, National Intelligence Law 2001, No. 25520, Article 4.
28. Law on the National Security of Romania, Article 21.
29. Canada, Privacy Act, R.S.C., 1985, Chapter P-21, Section 10. An overview of the personal information databanks maintained by the Canadian Security and Intelligence Services can be found at http://www.infosource.gc.ca/inst/csi/fed07-eng.asp.
30. The Netherlands, Intelligence and Security Services Act 2002.

31. For example, see the Netherlands, Intelligence and Security Services Act 2002, Article 47; Sweden, Act on Supervision of Certain Crime-Fighting Activities, Article 3; Switzerland, Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, Article 18 (1).
32. See for example, the Netherlands, Intelligence and Security Services Act, Articles 53–56; Croatia, Act on the Security Intelligence System, Article 40 (2) (3).
33. Ian Leigh, "Legal Access to Security Files: the Canadian Experience," *Intelligence and National Security* Vol. 12, No. 2 (1997), p. 126. For this study, interviews were conducted with officials of the Canadian Security Intelligence Service, the Information and Privacy Commissioners and their staff, users of the legislation, federal court judges, and other experts.
34. United Kingdom, Data Protection Act 1998, Section 28.
35. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: 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*, United Nations Document A/HRC/14/46 (17 May 2010), p. 23 (Practice 26).
36. Under Article 34 of the Intelligence and Security Services Act 2002, beginning five years after an intelligence service has exercised a special investigative power (and annually thereafter), "the relevant Minister will examine whether a report of the event can be submitted to the person with regard to whom one of these special powers has been exercised. If this is possible, this will take place as soon as possible."
37. Germany, Federal Act on Protection of the Constitution, Section 9.3.
38. The Netherlands, Review Committee on the Intelligence and Security Services (CTIVD), *Annual Report 2010–2011*, Chapter 4.
39. Germany, Act Restricting the Privacy of Correspondence, Posts and Telecommunications (G10 Act), (June 26, 2001), *Federal Law Gazette I*, p. 1254, revised 2298, last amended by Article 1 of the Act of July 31, 2009, *Federal Law Gazette I*, p. 2499, Section 12.1.
40. Germany, Federal Act on Protection of the Constitution, Section 9.3.
41. For example, see Germany, Federal Act on Protection of the Constitution, Section 14.2; Germany, G10 Act, Sections 4.1 and 5; Switzerland, Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, Article 15 (1) (5).
42. The Netherlands, Intelligence and Security Services Act 2002, Article 43; Croatia, Act on the Security Intelligence System, Article 41(1).
43. Germany, Federal Act on Protection of the Constitution, Section 12.2.
44. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: 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*, United Nations Document A/HRC/14/46 (17 May 2010), p. 22 (Practice 24).
45. Germany, Federal Act on Protection of the Constitution, Section 9.1.
46. Ibid., Section 13.
47. Ibid., Section 12.
48. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: 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*, United Nations Document A/HRC/14/46 (17 May 2010), p. 22 (Practice 25).
49. European Union, Charter of Fundamental Rights of the European Union, Article 8.3.
50. Sweden, Ordinance containing instructions for the Swedish Commission on Security and Integrity Protection, Sections 4–8 (on management and decision making) and 12–13 (on resources and support).
51. Hungary, Act on the National Security Services, Section 52.
52. *Al-Nashif v. Bulgaria*, No. 50963/99, ECHR, 2002, Paragraph 136.
53. *Association for European Integration and Human Rights v. Bulgaria*, No. 62540/00, ECHR, Paragraph 100.
54. Hans De With and Erhard Kathmann, "Parliamentary and Specialised Oversight of Security and Intelligence Agencies in Germany," in *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, Aidan Wills and Mathias Vermeulen (Brussels: European Parliament, 2011), Annex A, p. 220.
55. Norway, Instructions for Monitoring of Intelligence,

Surveillance and Security Services, Sections 11.1 (c) and 11.2 (d).

56. Iain Cameron, "Parliamentary and Specialised Oversight of Security and Intelligence Activities in Sweden," in *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, Aidan Wills and Mathias Vermeulen (Brussels: European Parliament, 2011), Annex A, pp. 279–81.
57. Sweden, Act on Supervision of Certain Crime-Fighting Activities (2007); see also Sweden, Ordinance containing instructions for the Swedish Commission on Security and Integrity Protection (2007) Section 2 (available at http://www.sakint.se/dokument/english/ordinance_instruction_scsip.pdf).

TOOL 7

Overseeing Information Sharing

Kent Roach

SEVEN

7

Overseeing Information Sharing

Kent Roach

1. INTRODUCTION

This tool examines the challenges posed by increased information sharing to the oversight of intelligence services and other branches of government that collect, analyze, and distribute national security information.[1] The term *information sharing* refers herein to information that is exchanged among intelligence services and partner agencies, whether they be foreign or domestic. Although the focus of this tool is principally on oversight bodies, it also considers the human rights and privacy implications of increased information sharing—which may be of interest to other entities such as the judicial and executive branches of government, the media, and civil society.

Intelligence services have always been tasked with sharing the information they collect. Since the terrorist attacks of September 11, 2001, however, much more emphasis has been placed on the sharing of information between intelligence services and between intelligence services and other entities on an international level. For obvious reasons, the increase in the amount of information sharing and the range of services involved has caused the problems associated with information sharing to increase. The information shared may be inaccurate, resulting in the misdirection of scarce resources by the recipient. Additionally, it may be put to inappropriate uses by the recipient service. In some extreme cases, it may even make services complicit in torture and other human rights abuses perpetrated by either the supplier or the recipient of the information.

Bad practices in information sharing can seriously harm the reputation of the providing state, as recent revelations of information sharing among Libyan, American, and British intelligence services have shown to be the case.[2] Even more consequential is the drastically harmful effect that inappropriately shared information can have on the reputations of individuals. These regrettable consequences make it especially important that information-sharing practices be subject to effective oversight, even though the information being shared is often highly classified. Oversight of information-sharing practices is particularly important given that these activities are normally conducted in secret and hence not easily reviewed in the courts or the media. Those who may be adversely affected by shared information may not even know that they have been affected and may be unable to make a complaint. In general, oversight bodies need to be given access to shared information. Otherwise, they will not be able to review effectively the information-sharing practices of the intelligence services that they oversee. However, the recent intensification of information sharing, as well as the secrecy of information being shared, presents challenges for oversight bodies that cannot be easily overestimated.

This tool begins with a brief examination of information sharing in the post-9/11 world. The main body examines the challenges to oversight of foreign and then domestic information sharing with regard both to the receipt and to the dissemination of information. The tool concludes with specific recommendations for improving information-sharing oversight. The recommendations address not only the policy, organizational, and managerial aspects of oversight but also legal frameworks within which information sharing can be more effectively governed.

2. INFORMATION SHARING

2.1 THE NEED FOR INFORMATION SHARING

It is obvious that both foreign and domestic intelligence services need to share information if they are to deal effectively with the complex security threats they face. In the current transnational environment, however, the need for even greater information sharing has frequently been emphasized. For example, in Resolution 1373 (28 September 2001), the United Nations Security Council specifically called for the intensification of information sharing among member states. In Europe, institutions such as Europol, the Club of Berne, the European Union Military Staff, and the European Union Situation Centre have also pushed for increased information sharing.[3] As a result, countries with very different traditions, which might otherwise be unwilling to engage with one another in joint security operations, are nonetheless prepared now to share information relating not only to counterterrorism but also to military and peacekeeping operations, weapons inspections, and war crimes prosecutions.

The extent of the information sharing currently taking place among intelligence services is difficult to gauge because the information is secret and so are the arrangements by which it is shared. The data that is available, however, provides some sense of scale. The Canadian and Australian domestic intelligence services, for example, each exchange information with about 250 foreign agencies. The American Central Intelligence Agency (CIA) is connected to more than 400 agencies worldwide.[4] This sharing occurs both formally and informally.

Because of the multifaceted nature of the current threat environment, countries that respect human rights may at times feel pressured to exchange information with nations that have poor human rights records. A service may believe that it must warn a country about a suspected terrorist who has entered or plans to enter a country, even though the country receiving the information may have a history of human rights abuse. It is also the case that information providers understandably come to expect a certain degree of reciprocity from information recipients.

In the decade since 9/11, many national governments have worked to eliminate legal and organizational barriers to information sharing among domestic agencies charged with security and intelligence responsibilities. This has been particularly true in the United States, where a governmental commission determined that barriers between intelligence and security agencies may have prevented the identification of some of the 9/11 hijackers.[5] As a result, the new zeal for information sharing has extended well beyond counterterrorism to a wide array of law enforcement responsibilities including border security, immigration, smuggling, and espionage.

2.2 PROBLEMS CAUSED BY INFORMATION SHARING

Although there is wide agreement that information sharing is necessary for increased security, the recent expansion of information sharing has raised a number of potential problems that require vigilant management and oversight. For example, law enforcement agencies are now more likely to undertake enforcement actions based on shared information that is unreliable, and there is now a greater risk that information shared by intelligence services will be disclosed in subsequent legal proceedings. Individuals are also at greater risk of having their rights, especially their right to privacy, infringed. Individuals will rarely have the opportunity to challenge the accuracy of shared information because they will often be unaware that information about them has been shared and will not have access to the shared information.

In many countries, intelligence services have been traditionally reluctant to share secret information with police and other law enforcement agencies. A commission of inquiry in Canada concluded that such reluctance contributed to the success of the 1985 Air India bombings and also to various deficiencies in the post-bombing investigation.[6] Intelligence services tend to guard information because they fear sharing it will result in its ultimate disclosure, which may expose important sources and methods and threaten the service's ability to collect intelligence in the future. Furthermore, if the information was obtained in a manner that makes it inadmissible in a legal proceeding, sharing it with law enforcement may be even more problematic. Police forces, while being perhaps more willing than intelligence services to share information, also worry that sharing information will disrupt their own ability to investigate and prosecute security threats.

Those charged with overseeing intelligence services face some of the greatest challenges of all. They must keep up with the vast amount of information now being shared, the volume of which is so great that they are regularly forced to rely on audits examining only a subset of the information. Most oversight bodies also encounter difficulties gaining access to and following the trail of secret information that is shared. For example, an oversight body with jurisdiction over the police may lack the authority to find out how information obtained by the police from an intelligence service was collected. This is especially true when the information provider is a foreign agency.

In many jurisdictions, networks of intelligence and security services (sometimes called "fusion centres") have been created to aggregate information about security threats provided by multiple domestic and foreign sources. Some of these networks even allow foreign agencies to exchange information with one another. Domestic oversight bodies need access to the information collected and distributed by these networks if they are to understand fully the operations of the agency they are mandated to oversee—especially as the agency provides information to and receives information from such regional, national, and supranational institutions.

One response to increased information sharing both among domestic agencies and with foreign agencies has been to appoint ad hoc inquiries with special jurisdiction to examine information sharing among multiple agencies. Boxes 1 and 2 will examine examples of such *ad hoc* inquiries in Canada and the United Kingdom.

Intelligence services have an obvious need to share information with domestic and foreign partners. A service that simply collects intelligence without sharing it would fail in its duty to warn others of the security threats it detects. The transnational nature of many current threats makes it necessary to increase the sharing of information both domestically and internationally.

Increased information sharing, however, is not without its drawbacks. It can lead to infringements of the right to privacy and other human rights in ways that are neither legally authorized nor ethically justified. It also risks the disclosure of secret information obtained from sensitive sources.

The sharing of information through domestic and supranational networks (fusion centres) can diffuse and distort accountability. Parliamentary and expert oversight bodies whose mandate limits their jurisdiction to a single agency often lack access to the records of the networks in which intelligence services take part—a lack of access that can seriously impede their oversight work.

Information sharing across national boundaries can also cause policy conflicts, such as when countries with good human rights records find themselves pressured into exchanging information with countries possessing poor human rights records. Exchanging information in this way can make one state complicit in human rights abuses, such as torture, conducted by its information sharing partner.

In short, intelligence services would not be doing their jobs if they refused to share information altogether; yet increased information sharing poses many risks. Those to individuals include abuses of human rights, especially the right to privacy. The risks to intelligence services include the dissemination of unreliable and/or improperly obtained information that can damage a service's reputation and result in the misallocation of scarce resources. The risks to oversight bodies include new limitations on their ability to understand what information is being shared and how that sharing is taking place.

Box 1: Ad hoc Canadian inquiries into information sharing

According to the reports of two multiyear Canadian commissions of inquiry (the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar and the Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin), the information-sharing practices of Canada's police and intelligence services indirectly contributed to the torture of Canadian citizens detained in Syria and Egypt on suspicion of terrorism.[7] Both commissions were ad hoc bodies appointed by the government primarily in response to public scandals but also because of a growing recognition that existing oversight institutions, tethered as they were to particular agencies, lacked the jurisdiction to examine how the whole of government responded to broad international security issues.

Both commissions asked the American, Egyptian, and Syrian governments to cooperate with their inquiries. All three foreign governments failed to do so. In addition, the Canadian government placed restrictions on the ability of both commissions to make public secret information that came into their possession. However, because these restrictions were subject to judicial review, the commissions were able in some cases to release more information than the government wanted—either through successful litigation or the prospect of such litigation. The commissions examined in some detail the information that Canada had shared with US, Syrian, and Egyptian officials. This information included intelligence linking various Canadians to terrorist groups. Specifically, it included lists of questions sent by Canadian officials to Syrian and Egyptian officials so that the questions could be put to Canadian citizens detained in Syria and Egypt on suspicion of terrorism.

The Canadian commissions also examined information received from those foreign officials, which was subsequently distributed within Canada and introduced into at least one legal proceeding. Both commissions found deficiencies in the ways that this information was shared—not only among domestic police, security, customs, and foreign affairs personnel but also with foreign agencies.

These two inquiries focused primarily on the propriety of information sharing, especially the dangers it posed to such human rights as the right not to be subject to torture and the right to privacy. Nevertheless, it would be incorrect to infer that the commissions were opposed to increased information sharing. They simply wanted better controls and enhanced reviews. The Arar Commission concluded that "information sharing is vital, but it must take place in a reliable and responsible fashion. The need for information sharing does not mean that information should be shared without controls, particularly without the use of caveats. Nor does it mean exchanging information without regard to its relevance, reliability or accuracy, or without regard to laws protecting personal information or human rights."[8]

A third Canadian inquiry, which looked into the 1985 Air India bombing, examined information sharing from a somewhat different perspective. Considering the efficacy of information sharing (as opposed to its propriety), the Air India commission developed recommendations designed to remedy the reluctance of intelligence services to share information with police and other law enforcement agencies because of the risk of disclosure. All three of these commissions recognized the fundamental dilemma of information sharing: too little sharing threatens security; while too much sharing, especially when that sharing is undisciplined, threatens human rights.

Box 2: An ad hoc British inquiry into information sharing

In 2010, the British government launched an official inquiry (the Detainee Inquiry) into the extent of British involvement in the mistreatment of detainees held by other countries.

At the outset, a protocol was prepared that stipulated that the government would provide the inquiry with all relevant information unless the provision of such information conflicted with existing duties of confidentiality.[9] The protocol also contemplated that the cabinet secretary would ultimately decide which materials could be made public. The purpose of this provision was to ensure that no harm would be done to the public interest through the unwarranted release of information relating to national security, international relations, defence, and the economy. Such a process differs markedly from the process used by the three Canadian inquiries discussed elsewhere herein, because it lacks any provision for the judicial review of government objections to the disclosure of information. In light of these and other restrictions, several human rights organizations refused to participate in the inquiry.

In January 2012, the UK government discontinued the inquiry as a result of the ongoing delays caused by the need to await the conclusion of criminal investigations – into some of the activities that the inquiry was due to examine – before the inquiry could begin its work. While this extensive ad hoc inquiry had the potential to be an extraordinary exercise of oversight, the British government's reliance on such discretionary and transitory measures underscores the limitations of its permanent oversight structures.

3. OVERSEEING INFORMATION SHARING WITH FOREIGN AGENCIES

The sharing of information with foreign agencies generally presents the greatest challenges to oversight bodies and the greatest risks to human rights. Foreign agencies may include intelligence services, police services, and other branches of foreign governments with access to diplomatic channels of communication. They may also include supranational networks in which one or more of these agencies take part. One commentator has observed that in contrast to domestic information sharing, which can be subject to centralized control, "in the chaotic international realm…not all countries adhere to privacy norms or other basic liberties. The right to privacy is, therefore, at the mercy of each and every intelligence agency in the network."[10]

Other rights at risk include the right not to be subject to torture or other forms of cruel, unusual, or degrading treatment. As the Arar Commission in Canada observed, "sharing information from investigations in Canada with other countries can have a 'ripple effect' beyond Canada's borders, with consequences that may not be controllable from within Canada."[11] In a worst-case scenario, information sent to a foreign agency may be used by that agency in support of extrajudicial detention, torture, and even killings. Conversely, information received from a foreign agency may have been obtained through torture or be otherwise tainted.

For obvious reasons, intelligence and police services are generally ill informed about the sources and methods used to obtain information provided by foreign agencies. This presents a problem, because the sources and methods used affect both the reliability of

the information and the recipient's obligations to respect human rights. Similarly, providers of information are often ill informed about the uses to which a foreign agency may put the supplied information. Providing agencies sometimes attach caveats restricting the use of shared information, but the providers have no way of ensuring that foreign partners will heed the restrictions. International information sharing is sometimes subsumed by state sovereignty and the need to protect the secrecy of sources, methods, and uses of intelligence. Domestic oversight bodies may have jurisdiction over the sending agency or the receiving agency but not both when one of these is foreign. Thus in practice, it can oversee only one side of the exchange transaction.

3.1 BAD PRACTICES IN INTERNATIONAL INFORMATION SHARING

In recent times, the most notorious example of bad practice in international information sharing has been the Maher Arar case. Following the 9/11 attacks, field investigators with the Royal Canadian Mounted Police (RCMP) shared the contents of an investigative database with officials of the US government. None of the information was screened in advance for reliability or relevance, nor did the RCMP place any restrictions on its use. A Canadian commission of inquiry subsequently determined that this information likely played a role in Mr. Arar's detention by the United States and his subsequent rendition to Syria, where he was tortured. Significantly, the commission could not reach a definitive finding because neither the US government nor the Syrian government cooperated with the inquiry. Faced with assertions of state sovereignty, there is little an oversight body can do to plumb the depths of secret international information sharing. Nevertheless, both the Arar commission and a subsequent inquiry into the detention by Syria and Egypt of three other Canadians found that questions sent to the Syrian and Egyptian authorities by the RCMP and the Canadian Security Intelligence Service contributed to the torture of the detainees by Syrian and Egyptian operatives.

Such findings present important cautionary tales as to what must be avoided. They warn that intelligence services, even when faced with urgent circumstances, must screen information before providing it to foreign partners. They must also, as necessary, attach caveats to the information and place restrictions on its use. Furthermore, they should refrain from sending follow-up investigatory requests, such as lists of questions, to foreign partners whose interrogators are known to engage in torture or other forms of human rights abuses.

3.2 GOOD PRACTICES BY INTELLIGENCE SERVICES IN INTERNATIONAL INFORMATION SHARING

What is good practice with respect to international information sharing? To begin, sharing agencies should make sure that they are well informed about their information partners. The UN special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has recommended that "before entering into an intelligence-sharing agreement or sharing intelligence on an ad hoc basis, intelligence services undertake an assessment of the counterpart's record on human rights and data protection, as well as the legal safeguards and institutional controls that govern the counterpart. Before handing over information, intelligence services [should] make sure that any shared intelligence is relevant to the recipient's mandate, will be used in accordance with the conditions attached and, will not be used for purposes that violate human rights."[12] Although the special rapporteur addressed this recommendation to

intelligence services, it also has relevance for oversight bodies, whose duty it is to ensure that good practices are followed and that remedies are provided for any failure to do so.

The Arar Commission found that the RCMP did not have adequate information about the practices of the Syrian and Egyptian security forces when it chose to share information with them. In general, among agencies that share information internationally, police forces have the least expertise in judging the practices of foreign partners. It would be prudent, therefore, for domestic agencies that share security information internationally to create and maintain a common database of current knowledge about potential foreign partners. In this way, domestic agencies could make informed decisions about specific information sharing. Such an approach would improve decision making with regard not only to sending information but also to assessing received information. In the Canadian cases cited previously, information derived from brutal interrogations was subsequently distributed widely among law enforcement, intelligence, and foreign policy officials. As the Arar Commission concluded, "It makes no sense to have different agencies operating on different assessments of information received from a foreign government."[13]

Also as discussed previously, it is imperative that intelligence services attach caveats to the information they provide to foreign entities, placing appropriate restrictions on its use. Although there is no guarantee that foreign governments will respect these caveats, there are good practices that can increase the likelihood they will be heeded—and, if they are not, such practices can also improve the chances that breaches will be remedied. The Arar Commission made several recommendations in this regard. First, caveats should be worded as clearly and precisely as possible. For example, permitting a receiving government to share information within its "intelligence community" allows the recipient too broad a mandate given the many agencies that can be fit within such a vague term. Second, receiving governments should generally be prohibited from using shared information in legal proceedings, whether they be criminal proceedings or proceedings related to immigration or extradition. Moreover, a caveat should always be attached requiring receiving governments to contact particular officials in the sending government should the receiving government wish to amend a caveat or report an abuse. This would replace the current bad practice of referring such matters vaguely to the sending agency or sending government, and it would promote individual accountability. According to the Arar Commission, "a caveat can serve to establish proper channels for clear communication about the use and distribution of the information subject to the caveat."[14] Finally, a caveat should always be included that requires the receiving agency to respect controls on personal information imposed by the laws of the sending jurisdiction as well as the controls that apply in the receiving jurisdiction.[15]

Should an intelligence or security service learn that one of its caveats has been breached, it should make an immediate complaint to the breaching agency. Depending on the severity of the abuse, the sending agency may need to reconsider the justifiability of the underlying information-sharing arrangement. At the same time, oversight bodies should be made aware of each breach and the sending agency's response. Oversight bodies can play an important role in ensuring that the agencies they oversee demand respect for caveats and take appropriate remedial action when necessary.

As suggested by the findings of the Arar Commission, special care should be taken when sending questions to foreign agencies, not only because they may invite the use of harsh interrogation tactics but also because foreign agencies may use such questions in a way

that is even less amenable to control by caveat. "Information," the Arar Commission concluded, "should never be provided to a foreign country where there is a credible risk that it will cause or contribute to the use of torture."[16] The UN special rapporteur has made a similar recommendation, emphasizing that oversight bodies should be especially attentive to conduct that might violate human rights. In addition, he has recommended that employees of intelligence services ordered to participate in conduct that violates human rights norms should be authorized to refuse those orders and to make complaints to oversight bodies.[17]

Information sharing with foreign partners should always be well documented because of the risks involved and also to facilitate review and oversight. Section 17 of the Canadian Security Intelligence Services Act gives the minister of public safety (in consultation with the minister of foreign affairs) the legal authority to enter into cooperation agreements with foreign agencies and governments. In the absence of such an agreement, CSIS cannot legally provide information to a foreign entity. (It can, however, receive information.)[18] A supplementary ministerial directive requires the RCMP to enter into specific written agreements with its information partners. These agreements are to be supported by legal—and, in the case of foreign agencies, foreign policy—advice. Even so, the Arar Commission found that the RCMP failed to apply this directive to day-to-day information sharing. The commission concluded that even though written agreements "need not be unduly formal or lengthy," they can increase the agencies' sensitivity to the need to respect caveats and human rights when sharing information.[19]

Audit trails are of particular importance when a intelligence service enters into a cooperation agreement with a foreign partner possessing a questionable human rights record. When information is provided to such a partner, the Arar Commission recommended, the providing agency should create a written record describing the information shared and the basis for the decision to share it.[20] The commission further recommended that a similar approach be employed when receiving information from countries with questionable human rights records:

> *In terms of accountability, it is important that the decision-making process be clearly described in writing and that those responsible for making the decision be identified. Furthermore, decisions to receive information from countries with questionable human rights records should be reviewed by the appropriate review body.*[21]

3.3 GOOD PRACTICES BY OVERSIGHT BODIES IN INTERNATIONAL AGENCY-TO-AGENCY INFORMATION SHARING

It is vitally important that oversight bodies have access to the information being shared by the agencies they oversee—whether or not that information is subject to claims of secrecy. Among the good practices recommended by the UN special rapporteur is that "independent oversight institutions are able to examine intelligence sharing arrangements and any information sent by intelligence services to foreign entities."[22] In fact, according to the UN special rapporteur, "it is good practice for national law to explicitly require intelligence services to report intelligence-sharing to an independent oversight institution."[23]

A potential barrier to effective oversight is the third-party rule, a common caveat placed on shared information that restricts its distribution to other entities ("third parties"). Some countries, such as Germany, do not grant oversight bodies access to shared information because they consider oversight bodies to be third parties.

A robust response to this interpretation of the third-party rule would be for oversight bodies to insist that, with regard to foreign information sharing, they be considered part of the intelligence service that receives foreign information. Intelligence services may resist such a position, fearing that it will make foreign services less willing to share information with them. But they can be encouraged to educate their foreign partners about the responsibilities they have to cooperate with oversight bodies, which in many cases follow the same secrecy procedures as the receiving agency.

Oversight bodies must also be mindful that intelligence services sometimes use information sharing as a means of avoiding domestic restrictions on their activities. Addressing this problem, the UN special rapporteur has proposed a good practice based on a report by the European Parliament on the ECHELON system of signals intelligence—specifically, that "intelligence services are explicitly prohibited from employing the assistance of foreign intelligence services in any way that results in the circumvention of national legal standards and institutional controls on their own activities."[24]

Finally, oversight bodies should adopt and/or encourage the same good information-sharing practices recommended to the intelligence services in their charge. For example, oversight bodies should inform themselves about the human rights records of foreign partners. Similarly, they should encourage the agencies they oversee to enter into formal written agreements with foreign partners.

Box 3: Oversight of foreign information sharing by the Dutch Review Committee on the Intelligence and Security Services

In 2002, the Dutch government created a permanent body with oversight responsibility for a wide range of intelligence matters, including jurisdiction to review the operations of several intelligence services and access to the secret information necessary to conduct such reviews. In 2009, this Review Committee on the Intelligence and Security Services issued an extensive report on Dutch cooperation with foreign services that focused on the policies and practices of a single Dutch intelligence service between 2002 and mid-2005.

The report found that the Dutch service and its foreign affairs department had been insufficiently attentive to whether foreign partners, including those with poor human rights records, met an appropriate standard for information sharing. The report also found that Dutch intelligence services had acted unlawfully in providing personal information to foreign partners. It recommended that these services cease sharing information with foreign partners whom they suspect might use the information for unlawful purposes.[25] The report also recommended putting in place a structured process for determining whether or not to enter into information-sharing agreements with foreign services. Such agreements would be subject to periodic review and would mandate that written records be kept of all personal information shared.[26]

3.4 GOOD PRACTICES BY OVERSIGHT BODIES IN INTERNATIONAL INFORMATION SHARING THROUGH NETWORKS

Because international information sharing can take place multilaterally as well as bilaterally, oversight bodies need to position themselves so that they can minimize the challenges and maximize the opportunities that come with sharing information across networks. For example, information-sharing networks can conduct human rights assessments of partner

agencies in a way that may be preferable to relying on individual member agencies to make the same assessments. Networks can also exercise greater influence than individual agencies when it comes to enforcing the human rights and privacy caveats that accompany many information exchanges.[27] Finally, networks have the potential to spread good practice with regard to information reliability and oversight by requiring member agencies to meet the standard set by those members with the best practices.

Some European information-sharing networks, such as those managed by Europol and the Club of Berne, have indeed imposed high standards, and these have proven to be beneficial. However, they have also encouraged some states to resort to less formal (and even case-by-case) bilateral information sharing.[28] To counter this tendency, oversight bodies should employ a two-track approach, emphasizing the benefits of sharing information within multilateral networks while at the same time paying close attention to the information exchanges that take place under less transparent bilateral arrangements. Although acquiring information about the foreign partners with which a domestic intelligence service shares information can be difficult, oversight bodies need to obtain this information and monitor foreign information-sharing agreements and practices.

For developing countries, the resources available to members of international information-sharing networks provide a strong incentive to join, even if joining mandates compliance with certain human rights standards. Oversight bodies can play an important role in promoting membership by making themselves aware of the standards that need to be met and encouraging the intelligence services they oversee to meet them.

4. OVERSEEING INFORMATION SHARING WITH DOMESTIC AGENCIES

As discussed previously, following the 9/11 attacks, many governments have increased information sharing among domestic partners—including intelligence, police, border, customs, and transportation officials—believing that such increased sharing will help prevent future terrorist attacks. In the United Kingdom, for example, Section 19 of the Terrorism Act of 2008 granted UK intelligence services broad latitude with regard to information sharing. It specifically authorized the disclosure of information to intelligence services by any person. It also authorized intelligence services to disclose information as necessary for the proper discharge of their functions, for the prevention or detection of serious crimes, and for the purpose of furthering criminal proceedings. In this way, the recent pressure to increase information sharing has resulted in greater disclosure relating not only to potential security threats but also to crime prevention and criminal investigations.

4.1 CHALLENGES OF DOMESTIC INFORMATION SHARING

From an oversight perspective, the disclosure of information to domestic partners raises many of the same concerns discussed above in relation to international information sharing. There are some additional concerns, however, that relate specifically to domestic information sharing. The most important of these is the danger that jurisdictional limitations may prevent the effective, coordinated review of domestic information sharing because the oversight bodies involved do not have the legal authority to review all of the

domestic agencies involved. When oversight powers are lacking in this way, accountability is diluted, and gaps are created in which information exchanges can take place without adequate review.

Because intelligence services possess special powers, national governments typically subject them to a higher degree of oversight than that imposed on law enforcement agencies. When accountability gaps occur, this enhanced oversight can be undermined. For example, when the Canadian government decided to investigate the actions of Canadian officials with regard to the torture of Maher Arar and other Canadians in Syria and Egypt, it found that the oversight jurisdiction of the permanent Security Intelligence Review Committee did not extend to the police, customs, foreign affairs, and immigration officials who had been involved in the information sharing with Syria and Egypt. As a result, it had to create impermanent, ad hoc inquiries to fill the accountability gap.

Federalism can also lead to dangerous accountability gaps. In the United States after 9/11, for instance, fusion centres were created to promote the sharing of information among federal, state, and municipal agencies. Advocates insisted that no new oversight mechanisms were necessary because each participating agency remained subject to a pre-existing oversight structure. This argument failed to recognize, however, that as a practical matter oversight bodies associated with one level of government rarely have the jurisdiction necessary to review the actions taken by agencies on other levels of government.[29]

4.2 BAD PRACTICES IN DOMESTIC INFORMATION SHARING

Since 9/11, an especially bad practice in domestic information sharing has been the misidentification of non-violent protesters as terrorism suspects. In the United States, several fusion centres have been guilty of this practice. Because the misidentification occurred after various databases provided by federal, state, and local agencies were merged with strategic information relating to terrorist threats and vulnerabilities, the participating agencies either claim ignorance or blame someone else for the unreliable information. Some fusion centres have compounded the problem by refusing to provide oversight bodies with records describing how the information was assembled.[30] These factors combine to make it very difficult to hold fusion centres and their contributing agencies to account for their activities.

More generally, information networks and the agencies that belong to them need to reduce the indiscriminate sharing of potentially unreliable information. In Canada, unreliable information obtained from a foreign agency by the Department of Foreign Affairs was subsequently distributed to domestic intelligence and law enforcement agencies without any concerns as to its reliability being noted. It was even used as a basis for obtaining a search warrant. In this way, bad practices in domestic information sharing can multiply the dangers inherent in foreign information sharing.

4.3 GOOD PRACTICES IN DOMESTIC INFORMATION SHARING

Good practice in domestic information sharing begins with the keeping of permanent records that track the information held and shared by fusion centres and other entities facilitating information exchange. Without such record keeping and the audit trails it permits, oversight of domestic information sharing would be difficult, if not impossible.

Caveats are also as good a practice in domestic information sharing, as they are in international information sharing, especially when the information being shared is to be used in connection with law enforcement. The sharing agency needs to consider carefully whether the information being shared is reliable enough to be used for enforcement purposes and also whether the agency has the legal right to share the information for that purpose. The UN special rapporteur has emphasized the need for countries to enact legal bases for domestic information sharing. Section 19 of the UK's Terrorism Act of 2008 provides one such example.

The creation of a legal basis can provide legislators with an opportunity to reflect on the adequacy of oversight mechanisms currently in place and perhaps make changes to the current oversight structure. For example, while considering the legal basis for Canadian oversight, the Arar Commission recommended that the Canadian legislature create "statutory gateways" allowing different oversight bodies to share secret information and work together in reviewing national security activities. The commission's recommendation was based on the sound principle that oversight should keep pace with the activities being overseen. In other words, if the statutory authorization for information sharing is being expanded, so, too, should review powers.

Commentators have argued that a distinct form of "network accountability" is necessary if oversight bodies are to keep pace with the proliferation of domestic information-sharing networks. Recommendations include the recording and preservation of all shared information (so that oversight bodies can compile tamper-resistant audit trails) and the establishment of redress mechanisms within fusion centres (so that dissemination of inaccurate information and violations of privacy rights can be corrected).[31] Other commentators have emphasized the need for inspectors general, especially in the United States, to conduct joint inquiries into the information-sharing practices of the agencies that they oversee.[32] In Canada, the Arar Commission similarly recommended that the jurisdiction of intelligence oversight bodies be expanded to include a number of agencies that took on significant new security responsibilities after 9/11.[33] In Belgium, the separate bodies that oversee police and intelligence services, respectively, are already permitted to share information, and they have also conducted several joint investigations.[34]

In the absence of such broad oversight arrangements, governments wishing to investigate the actions of multiple domestic agencies engaged in security information sharing must establish ad hoc inquiries such as the Arar Commission because no existing oversight body possesses the necessary mandate to review the actions of multiple agencies. The appointment of an ad hoc body, however, being discretionary and extraordinary, is no substitute for a permanent oversight body with sufficient authority to carry out meaningful review. For this reason, the Arar Commission recommended that the permanent oversight bodies charged with reviewing the actions of Canada's intelligence and law enforcement agencies be granted greater authority to review the actions of a number of agencies with which security information is shared. Unfortunately, this recommendation and the recommendation that the government create statutory pathways for joint oversight—both of which were made in 2006—have yet to be implemented.[35]

In the United States, some progress has been made toward investing permanent accountability structures with the capacity to examine the multiple domestic agencies that now take part in security information sharing. One example is the inquiry into warrantless wiretapping conducted jointly by the inspectors general of the Department of Defense,

the Department of Justice, the Central Intelligence Agency, the National Security Agency, and the Office of the Director of National Intelligence.[36]

Box 4: Review of domestic information sharing by an inquiry into Australian intelligence services

Australia has made significant progress in adapting intelligence oversight to meet the emerging whole-of-government approach to security issues and information sharing. An Australian inquiry into intelligence recommended in 2006 that the inspector general, an expert oversight body, and the relevant parliamentary joint committee have their mandates expanded to allow them to oversee the actions of all domestic intelligence services.[37]

Although this recommendation recognized the expansion of information sharing among domestic intelligence services, it paid less attention to the information sharing between domestic intelligence services and other domestic agencies. This deficiency was corrected in 2010, when the Australian parliament enacted legislation that granted the inspector general the authority to examine all matters related to security and intelligence within any federal department or agency.[38] In one respect, however, the new legislation was less than desirable. Although the UN special rapporteur has emphasized the importance of oversight bodies being able to initiate their own reviews, the new Australian legislation required a mandate from the prime minister to trigger the inspector general's expanded powers.[39]

Meanwhile, Australia has created new parliamentary committees to review the actions of law enforcement agencies involved in national security and information sharing. It has also increased the size of the joint parliamentary committee charged with the oversight of intelligence services.

5. RECOMMENDATIONS

The following recommendations are intended to facilitate the oversight of domestic and international information sharing. They are addressed not only to oversight bodies in the legislative and executive branches of government but also to the intelligence services being overseen and to various other entities involved in whole-of-government responses to security threats.

Given that information sharing must occur, it needs to be conducted in a manner that is legally authorized and respectful of human rights, including the right to privacy. An important means of ensuring this is to provide oversight bodies with the legal and other resources they need to keep pace with the increased intensity of domestic and international information sharing in the post-9/11 world.

Developing internal guidelines on information sharing

Intelligence services should devise a set of principles to govern their information-sharing practices. These principles should be set forth in written form, either as law or policy. They should:

- mandate respect for human rights (including the avoidance of complicity in torture) and respect for laws governing privacy (including the sharing of personal information).

In particular, the principles should prohibit the sharing of information when there exists a credible risk that the information exchange will cause or contribute to the practice of torture.

- require the screening of shared information (whether it is being sent or received) for relevance, reliability, accuracy, and impact on privacy and other human rights.
- recognize the need to attach caveats to information being sent and to respect caveats placed by others on information being received—the purpose of such caveats being to ensure that shared information is not used for improper purposes or in an improper way that violates domestic or international law.
- acknowledge a continuing obligation to correct erroneous information sent to other agencies and to conduct independent assessments of the reliability of information received from others.
- include a commitment to sharing information in a manner that facilitates accountability within the sharing service and with respect to oversight bodies. That is, the shared information should be recorded in writing, and audit trails should include descriptions of how the information exchange was authorized and of any follow-up actions. If information sharing takes place without such authorization—at the field level, for example, or under exigent circumstances—it should be clearly explained in writing at the earliest opportunity.

Intelligence services should incorporate these principles into their training programmes and share them with oversight bodies. They should also make them available to the public, provided that they do not raise national security confidentiality concerns. If an intelligence service fails to develop these principles, its oversight body should develop similar principles and apply them to the work of oversight.

Developing an informed approach to information sharing within an intelligence service

Intelligence services should maintain databases that track the human rights records of countries with which they share information. These databases should:

- include a broad range of open information, including allegations of human rights violations made by international and regional rights-protection bodies and by credible civil society groups.
- be developed in consultation with foreign affairs departments.
- be used to train intelligence service personnel.
- be made available to the public in a manner consistent with national security confidentiality concerns.

Oversight bodies should have access to these databases—which they should review and, as necessary, supplement and update. If an intelligence service fails to create such a database, its oversight body should do so.

Developing international information-sharing agreements

Intelligence services should develop written agreements to govern the sharing of

information with foreign partners. These agreements should specify the obligations of both sending and receiving parties with regard to human rights. They should also include standard clauses that permit received information to be shared with the service's principal oversight body and, when possible, with related oversight bodies that agree to the same confidentiality protocols. In constructing these agreements, the intelligence service should obtain both legal and foreign policy advice.

Oversight bodies should receive copies of all such agreements at the time they are entered into or when they are revised. The oversight body should be obliged to review each agreement and, when possible, undertake random audits to measure compliance with the terms of the agreement. Such audits can help determine whether the agreement needs to be revised in light of past practice.

Reporting and resolving breaches of caveats placed on shared information

Information-sharing agreements should include specific procedures for the reporting of breaches of caveats placed on shared information by the sending party and the resolution of disputes arising from breaches of caveats. If a sending agency becomes aware of a breach, it should issue a formal objection to the receiving agency. The sending agency should also use the occasion as an opportunity to reconsider the applicable information-sharing agreement and possibly make changes. Such a procedure could also be used to correct or update information and to propose amendments to caveats in specific cases or over time.

In the event of a breach (or even a suspected breach), intelligence services should notify their oversight bodies. Such notification should include a log of any remedial actions the service has taken or proposes to take. The oversight body should review and comment on all remedial actions and also address the overall question of how the breach should affect future information sharing with the breaching partner.

Reporting and resolving the illegal use of shared information

Intelligence services should notify their oversight bodies when they become aware (or even suspect) that shared information was obtained or has been or may be used illegally, especially in connection with human rights violations. Such notification should include a log of any remedial actions the service has taken or proposes to take. The oversight body should review and comment on all remedial actions and also address the overall question of how the illegality should affect future information sharing with the violating partner.

Developing domestic information-sharing agreements

Intelligence services should develop written agreements to govern the sharing of information with domestic partners. Such agreements should:

- have unambiguous legal authorization.
- address caveats as well as human rights compliance.
- provide for clear audit trials (including permanent records of all information shared and written authorizations from both the sending and receiving agencies).
- address how domestic information sharing will be reviewed by the relevant oversight bodies.

In constructing these agreements, the intelligence service should obtain legal advice, especially with regard to privacy and other legal restrictions on information sharing. The legal advice should also address the question of whether the jurisdiction of the agency's oversight body is sufficient to review its information-sharing practices.

In addressing accountability issues, these agreements need to foresee and resolve problems created by the fact that sending and receiving agencies may be subject to different oversight regimes. Whenever possible, oversight bodies should be granted access to all information necessary for the effective review of information-sharing practices. This may require further legal authorization for domestic oversight bodies to carry out joint reviews and to share information among themselves. It may also require oversight bodies to abide by more stringent security and secrecy measures than is usually their practice.

Endnotes

1. The term *intelligence service* is used herein to mean a government organization whose main tasks are the collection and analysis of national security–related information and its dissemination to decision makers. This definition has been taken from Aidan Wills, *Guidebook: Understanding Intelligence Oversight*, Toolkit—Legislating for the Security Sector (Geneva: DCAF, 2010), p. 10.
2. BBC News, "Libya: Gaddafi regime's US-UK spy links revealed," September 3, 2011 (available at http://www.bbc.co.uk/news/world-africa-14774533).
3. James Walsh, "Intelligence-Sharing in the European Union: Institutions Are Not Enough," *Journal of Common Market Studies* Vol. 44, Issue 3 (September 2006), pp. 625–643.
4. Elizabeth Sepper, "Democracy, Human Rights and Intelligence Sharing," *Texas International Law Journal* Vol. 46 (2010), p. 155.
5. Ernest R. May (ed.), *The 9 /11 Commission Report* (New York: St. Martins Press, 2007), Section 3.2.
6. Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Air India Flight 182: A Canadian Tragedy* (2010).
7. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006); and Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin* (2008).
8. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), p. 331.
9. Detainee Inquiry, "Protocol for the Detainee Inquiry" (2011) (available at http://www.detaineeinquiry.org.uk/key-documents/protocol/).
10. Francesca Bignami, "Toward a Right to Privacy in Transnational Intelligence Networks," *Michigan Journal of International Law* Vol. 28, No. 3 (Spring 2007), p. 674.
11. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (2006), p. 431.
12. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: 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*, United Nations Document A/HRC/14/46 (17 May 2010), p. 46.
13. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), p. 349.
14. Ibid., p. 342.
15. Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practices for Oversight of Intelligence Agencies* (Geneva: DCAF, University of Durham, and Parliament of Norway, 2005), p. 45.
16. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), p. 345.
17. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: 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*, United Nations Document A/HRC/14/46 (17 May 2010).
18. Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin* (2008), p. 82.
19. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), p. 322.
20. Ibid., p. 347.
21. Ibid., p. 348.
22. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: 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*, United Nations Document A/HRC/14/46 (17 May 2010), p. 48.
23. Ibid., p. 49.
24. Ibid., pp. 49–50.
25. The Netherlands, Review Committee on the Intelligence and Security Services (CTIVD), *Review*

Report on the cooperation of the GISS with foreign intelligence and/or security services, CTIVD No. 22A (12 August 2009) (available at http://www.ctivd.nl/?English), Section 14.2.

26. Ibid., Sections 14.6 and 14.15.
27. Francesca Bignami, "Toward a Right to Privacy in Transnational Intelligence Networks," *Michigan Journal of International Law* Vol. 28, No. 3 (Spring 2007), pp. 683–684.
28. Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin* (2008), p. 68.
29. Danielle Citron and Frank Pasquale, "Network Accountability for the Domestic Intelligence Apparatus," *Hastings Law Journal* Vol. 62 (2011), p.1441.
30. Ibid.
31. Ibid.
32. Philip Heymann and Juliette Kayyem, Preserving Liberty in the Face of Terror (Boston: MIT Press, 2005); Kent Roach, "Review and Oversight of National Security Activities and Some Reflections on Canada's Arar Inquiry," *Cardozo Law Review* Vol. 29, Issue 1 (October 2007), pp. 53–84.
33. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (2006).
34. Ibid., pp. 333–334.
35. Kent Roach, *The 9/11 Effect: Comparative Counter-Terrorism* (Cambridge: Cambridge University Press, 2011), pp. 416–420 and 455–459.
36. Offices of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, and Office of the Director of National Intelligence, *Unclassified Report on the President's Surveillance Program* (10 July 2009).
37. Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies* (Canberra: Government of Australia, 2004).
38. Australia, National Security Legislation Amendment Act No. 127 of 2010, schedule 9; see also Kent Roach, *The 9/11 Effect: Comparative Counter-Terrorism* (Cambridge: Cambridge University Press, 2011), pp. 354–356.
39. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: 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*, United Nations Document A/HRC/14/46 (17 May 2010).

TOOL 8

Financial Oversight of Intelligence Services

Aidan Wills

EIGHT

8

Financial Oversight of Intelligence Services

Aidan Wills[1]

1. INTRODUCTION

In democratic countries, parliaments allocate treasury funds to public agencies so that the agencies can perform their functions and fulfil their legislative mandates. Parliaments then, in conjunction with other oversight bodies, monitor the expenditure of these funds to ensure that their use is both legal and efficient. All public agencies must submit to this process, including intelligence services.

This tool presents a comparative overview of how democratic polities oversee the finances of intelligence services, from the formulation of budgets through to the *ex post* review of expenditures. Its aim is to highlight good practices. It contains the following six sections:

- *the Importance of Financial Oversight of Intelligence Services*
  an explanation of why external oversight is important
- *Intelligence Budgets*
  an overview of different approaches to intelligence budgeting
- *Internal Financial Controls and Audit Mechanisms*
  an overview of controls and mechanisms that make external oversight more effective
- *Parliamentary Oversight*
  a discussion of the role of parliaments in formulating intelligence budgets, overseeing their implementation, and reviewing service expenditures for legality and effectiveness

- *Supreme Audit Institutions*
  a discussion of the role of supreme audit institutions (SAIs) in auditing the finances of intelligence services
- *Recommendations*
  a compilation of good practices relating to the financial oversight of intelligence services

For reasons of space, this tool does not address the roles played in the financial oversight of intelligence services by the executive, inspectors general, prosecutors, and the judiciary.

This tool defines "financial oversight" broadly, to include functions that may also be characterized as exercises of "control" (see Born and Geisler Mesevage—Tool 1) and take place before, alongside, or after the financial activities being overseen.

2. THE IMPORTANCE OF FINANCIAL OVERSIGHT OF INTELLIGENCE SERVICES

There are four main reasons why external oversight of intelligence service finances is important:

- The principles of democratic governance require the allocation and use of public funds to be closely scrutinized.
- Financial records can provide insights into the behaviour and performance of intelligence services.
- Intelligence service secrecy limits the ability of the public to scrutinize service activity.
- The nature of intelligence work creates a variety of financial risks, including the risk of the misuse of public funds.

2.1 DEMOCRATIC GOVERNANCE IN RELATION TO THE USE OF PUBLIC MONEY

A universally accepted principle of democratic governance is that the appropriation of public funds must be approved by the elected representatives of the people—that is, the parliament—because the money that is being appropriated belongs to the public. Parliaments use their budgetary powers to shape the policies and priorities of government entities to reflect the will of the public. Equally important is the tenet that public expenditures must be subject to *ex post* review by the parliament as well as by independent bodies reporting to the parliament (such as SAIs). The purpose of *ex post* review is to ensure, inter alia, that:

- Public funds were put to the uses for which they were originally appropriated.
- Expenditures comply with applicable law (including laws on the management of public funds, laws on public procurement, anticorruption laws, and laws governing the activities of the body concerned, e.g., an intelligence service).
- Expenditures were consistent with government policies.
- Expenditures provided value for money by accomplishing established aims in an effective manner.

Although these principles apply equally to all governmental agencies, including intelligence services, some countries explicitly exclude intelligence services from certain laws regulating the expenditure of public funds. One example is in the United States with regard to the Central Intelligence Agency (CIA).[2] In such cases, close scrutiny is particularly important.

2.2 FINANCIAL RECORDS AS INDICATORS OF BEHAVIOUR AND PERFORMANCE

A public agency's finances usually indicate a great deal about its activities and performance. Rarely can an agency perform a task without spending money. Therefore, its financial records will often contain clues to hidden activities, including some that may be illegal. In the case of intelligence services, illegal activities, such as the operation of secret detention facilities and the covert funding of domestic political parties, may be revealed in the service's financial records. Similarly, an unusually high departmental budget line might indicate poor performance on the part of that department. Thus, by examining the financial records of a service, oversight bodies can identify aspects of the service's work that may require further scrutiny.

2.3 SECRECY AND THE LIMITING OF PUBLIC SCRUTINY

Because intelligence work necessitates an unusually high level of secrecy, intelligence service finances are not disclosed to the same degree as those of other governmental agencies. Secrecy in the area of tenders for goods and services[3] is compounded by the exclusion of intelligence services from most laws regulating public access to state-held information, thereby limiting the amount of relevant information that the media and other civil society organizations can obtain. Given these limitations on public scrutiny, it is especially important that external oversight bodies possessing access to confidential information closely scrutinize intelligence service finances.

2.4 MANAGING FINANCIAL RISK IN INTELLIGENCE WORK

Particular aspects of intelligence work create a heightened risk that public funds will be used ineffectively or improperly. Many of these aspects also make intelligence oversight a very challenging task.

2.4.1 Uncertain outcomes

Intelligence services collect information to aid policymakers in protecting national security. To perform this function, services spend money; but they can never be certain that the money they spend will yield the information they seek. For instance, a service may spend a great deal of money recruiting a foreign informant only to discover that this informant possesses little information of value. Although such risks are inherent to intelligence work, internal controls and external oversight can manage them, minimizing the waste of public funds.

2.4.2 Intangible benefits

Although the financial costs of an intelligence operation are often tangible, the benefits that it produces are often intangible. As Canada's Auditor General has observed, "The

results—and particularly the ultimate effects—of intelligence collection, assessment and reporting are inherently difficult to measure."[4] This is especially true when the object of an operation is the non-occurrence of an event, such as a terrorist attack. Only an oversight body with sufficient knowledge and experience can properly evaluate the intangible benefits of an intelligence operation and determine whether it represents appropriate value for money.

2.4.3 Secrecy and the misuse of public funds

Intelligence services are understandably concerned that sensitive information, such as operational details and the identities of sources, remain confidential. Accordingly, they compartmentalize this information, limiting knowledge to as few people as possible, even among service personnel. However, the smaller the circle of knowledge, the greater the risk that public funds will be misused. For example, if information about an informant is limited to the intelligence officer "running" the informant, then there exists the opportunity for officers to create non-existent "phantom agents" for the purpose of embezzling the funds allegedly being paid to these agents. Even when informants are real, secrecy rules can make it easier for intelligence officers to keep for themselves money allocated to informants without much risk of detection.

2.4.4 Conflicts of interest

As part of their work, intelligence officers sometimes pay people secretly to provide them with information or to render services, such as the use of a house from which to conduct surveillance. Often, decisions on whom to pay and how much to pay are largely at the discretion of the officer (and perhaps a supervisor). This creates a potential conflict of interest because officers' decisions are likely to be based not only on the merit of the provider but also on personal connections and especially, given the confidential nature of the transaction, on the degree of trust the officer has in the provider. As a result, some officers may engage people simply because they are acquaintances. Officers may also pay excessive amounts because the provider is a close associate. In some cases, officers may even take kickbacks (see Box 1).

Box 1: The case of Kyle Foggo

Kyle Foggo once worked for the CIA as a senior intelligence officer. His responsibilities included the procurement of goods and services for highly sensitive operations, including the construction of secret overseas detention facilities. To procure material for some of these facilities, Foggo arranged for the CIA to contract with a company linked to a close friend of his. Prosecutors later determined that Foggo steered multiple contracts to this company, paying inflated prices for the goods and services provided. In return, Foggo received favours, including expensive holidays and promises of future employment. Concealing this relationship from colleagues, Foggo sought to justify his use of the company by claiming that he needed to procure the goods and services from a provider he could trust and that he also wanted to avoid the standard bureaucratic procurement procedure. Ultimately, Foggo pleaded guilty to corruption and served a prison sentence.[5]

2.4.5 Risks associated with disposable assets and income

Intelligence services purchase a significant number of disposable assets as part of their

operations. For example, they may buy expensive vehicles or use expensive hotels to enable an agent to associate with wealthy targets during an operation. Intelligence officers may seek to profit from such valuable goods once they are no longer needed by retaining them for personal use, passing them on to acquaintances, or selling them and retaining the proceeds. That these assets were procured secretly enhances the risk. Similarly, some intelligence services set up "front" companies to provide cover for covert activities. Some of these companies may generate income, creating the risk that the officers concerned may unlawfully retain the income for themselves. Because of these risks, oversight bodies must monitor not only intelligence service expenditures but also service assets and income.

2.4.6 Use of intelligence services for political purposes

Misuse of intelligence service funds can also extend to those members of the executive who are responsible for intelligence services. Such officials have at times used service resources for illegal political purposes involving the expenditure of public funds. Thus, oversight bodies need to focus not only on the behaviour of service officers but also on their interactions with executive officials.

3. INTELLIGENCE BUDGETS

A *budget* is an itemized document detailing planned revenues and expenditures for a forthcoming period of time, typically a fiscal year. As such, it is a key tool for directing and controlling the work of a public agency, because agencies need funding in order to function. In democratic countries, budgets are normally enacted by parliaments as pieces of legislation.

In some countries, intelligence services are organizationally autonomous, with budgets of their own. In other countries, they operate within ministries—such as the French ministry of the interior, which houses the French domestic intelligence service (la Direction Centrale du Renseignement Intérieur). In the latter case, the intelligence services do not have their own budgets. Instead, they are funded under the budget of the ministry to which they belong. Thus, the term *intelligence budget* can be a confusing one, sometimes referring to the budget of a single service and sometimes to the budget of multiple services within a single ministry. The term can also refer to aggregated amounts for an entire intelligence community across several ministries. It should also be noted that, in some countries, not all expenditure related to intelligence services is included their budgets. Notably, expenditure on pensions and items such as stationery might be included in other parts of the state budget. This can make it difficult to calculate the overall budget for intelligence services.

The organizational status of a service is important because of the implications it has for scrutiny of the service's budgets. As a general rule, external overseers can conduct more direct, detailed scrutiny of the finances of intelligence services that are established as autonomous agencies than the finances of intelligence services that operate within a ministry. This is because the finances of an autonomous service are not entangled with those of other ministerial departments.

The budgets of governmental agencies, whether those agencies perform intelligence work

or not, should be "comprehensive." The World Bank uses this term to mean that budgets "must encompass all fiscal operations."[6] In other words, the budget of a governmental agency should include all of the financial activity that relates to that agency.[7] Intelligence services, in particular, need to respect this requirement because some have a history of raising money for and spending it on activities not authorized by law. An example would be the CIA's use of revenue raised from Iranian arms to fund support for the Nicaraguan contras during the mid-1980s.

3.1 THE BUDGET CYCLE

The term *budget cycle* refers to the complete process by which money is requested, allocated, and spent (including the *ex post* review of such spending). There are four principal stages in the budget cycle:

- formulation, during which responsible ministries, government departments, and agencies determine planned revenues and expenditures
- scrutiny and approval, during which the parliament amends and enacts the budget
- implementation, during which the agency implements the plan detailed in the budget
- *ex post* review, during which oversight bodies scrutinize the agency's use of money; this may be followed by a parliamentary vote to "discharge" (approve and sign off) government accounts for a given year[8]

Although intelligence service budgets are formulated in much the same way as the budgets of other government departments and agencies, the procedures for their scrutiny and approval, implementation, and *ex post* review (discussed in Sections 5–6 of this tool) are different.

3.2 APPROACHES TO BUDGETING

Traditional budgeting uses the line-item method, allocating specific amounts (inputs) to costs or budget lines, without linking such inputs to policy objectives or outputs. In contrast to this input-based approach, many countries (such as France) are now using a "performance" or "results-based" budgeting method that links the allocation of funds to policy objectives and ultimately to desired outcomes.[9] The approach taken to budgeting has important implications for *ex post* oversight. Because results-based budgeting establishes links between inputs and outputs, it is easier to subsequently assess the implementation of a budget, including factors such as efficiency and value for money. By contrast, input-based budgeting does not provide a framework to assess the implementation of a budget.

3.3 PUBLICATION OF INTELLIGENCE BUDGETS

To the best of the author's knowledge, there is no government that makes public in their entirety the budgets of its intelligence services. In most countries, classified budget details are withheld not only from members of the public but also from members of parliament who do not belong to committees that are authorized to classified information in this domain.

The secrecy surrounding intelligence budgets is motivated by intelligence service concerns that publishing budgetary information will benefit their adversaries. However, this is likely to be true only if the published information contains details relating to specific targets,

methods, or sources of information. In most cases, far more information can be disclosed than is presently the case, posing no risk to national security yet greatly enhancing transparency.

In general, democratic countries choose among three approaches to the public disclosure of intelligence budgets. Some (such as the United Kingdom[10]) make public only the total amount allocated to the entire national intelligence community. Others (such as Germany) make public the individual total for each intelligence service. Obviously, neither of these approaches discloses any links between resources allocated and specific policy objectives—information that might usefully inform public debate. The third approach (employed by Australia and France, for instance) is to disclose the specific amounts allocated for particular purposes. For example, the publicly disclosed annual budget for the Direction Générale de la Securité Exterieure (DGSE), the French foreign intelligence service, lists authorized expenditures for personnel, operational costs, and investments separately; the total amount appropriated for special operational activities (*les fonds spéciaux*) is also made public.

Governments that employ performance budgeting (which Australia and France both do) may also disclose policy objectives and desired outcomes so that members of the public can see the links for themselves.[11] The public version of the 2010 DGSE budget, for example, established the "improvement of the DGSE's capacity to collect and analyse intelligence" as a core policy objective, citing the planned recruitment of 690 additional employees between 2009 and 2015 as a means of achieving this objective.[12]

Disclosing as much budgetary information as possible—which the third approach accomplishes better than the other two—is beneficial to society for several reasons. First, it respects the public's right to know how its money is being spent. Second, it enhances transparency—enabling rank-and-file parliamentarians (that is, parliamentarians who are not members of committees authorised to access classified information in this field), the media, and even members of the public to participate meaningfully in public debate on the funding, policies, and priorities of intelligence services. Robust public discussion compels governments to justify their spending priorities, which can ultimately promote the more efficient use of public funds. Finally, open debate enhances public confidence in the intelligence services, dispelling myths about the purposes of intelligence spending and even resulting at times in increased intelligence funding.

The decision on how much budgetary information to disclose should not be left to the executive alone. Parliaments should, through legislation, regulate what financial information may be kept secret and what must be disclosed. Regardless of how much budgetary information is made public, it is essential that parliamentary committees involved in scrutinizing, amending and/or approving intelligence budgets have access to all relevant information including classified sections of the budget (see Section 5.1).[13]

4. INTERNAL FINANCIAL CONTROLS AND AUDIT MECHANISMS

Although this tool focuses on the role that external oversight bodies play in monitoring intelligence service finances, its presentation would be incomplete without some

discussion of the internal financial controls that exist within intelligence services. Without such mechanisms in place, external oversight cannot be effective.

4.1 ACCOUNTING

The law normally requires all public agencies, including intelligence services, to designate an accounting officer—whose responsibility is to ensure that the agency keeps orderly, accurate financial records and that it complies with all applicable regulations (see Box 2). Often, the accounting officer is the director of the agency, who is supported in this role by a financial division that handles the day-to-day work of recording and reporting all of the agency's financial transactions. Financial divisions also establish and maintain financial controls to ensure that resources are being used properly.

Box 2: South African law on accounting officers

This box distills selected provisions of the South African Public Finance Management Act of 1999, which regulates internal financial controls for government agencies (including the intelligence services). In accordance with this law, South African accounting officers have broad responsibility for ensuring that their agencies employ good financial practices.

Every agency of the South African government must have an accounting officer who is responsible for:

1. ensuring that the agency maintains an effective, efficient, and transparent system of financial risk management, as well as an internal audit system under the control of an audit committee operating in accordance with applicable regulations
2. the effective, efficient, economical, and transparent use of agency resources
3. the management of agency assets and liabilities, including the safeguarding of agency assets
4. ensuring that agency expenditures comply with relevant budgetary legislation

The law further charges accounting officers with preventing and, if necessary, responding to unauthorized, irregular, or wasteful agency expenditures. When such an expenditure is discovered, the accounting officer must immediately report, in writing, the particulars of the expenditure to the treasury and, in the case of an irregular expenditure involving the procurement of goods or services, to the relevant tender board. In addition, the accounting officer must take appropriate disciplinary action against any official who undermines the agency's financial management system or who makes (or permits to be made) an unauthorized, irregular, or wasteful expenditure.

With regard to record keeping, the accounting officer must keep full and proper records of the financial affairs of the agency in accordance with prescribed norms and standards.

Proper internal accounting is essential to the work of external oversight bodies because, without it, SAIs and other such bodies would have great difficulty reconstructing transactions and associated activity. In general, the quality of an intelligence service's accounting is indicative of whether its financial records are fair and true.

4.2 GUIDELINES FOR FINANCIAL MANAGEMENT

Like all government agencies, intelligence services formalize their financial management and accounting procedures in a set of written guidelines. Normally issued by the service director or the executive and then assessed by an external oversight body, these guidelines make up part of the regulatory framework against which the actions of service employees are evaluated.

Typically, guidelines for financial management cover the following issues:

- By whom and through what process are revenue generation and expenditures authorized? In answering this question, the guidelines should establish clear lines of responsibility and accountability for financial transactions.
- What are the permissible uses of service funds? The answer to this question should be aligned with relevant legislation.
- How should financial transactions take place? The guidelines should advise, for instance, whether operatives should use cash or make electronic payments.
- What financial records should be kept? Proper record keeping is important because it establishes an audit trail for later use. However, in some countries, such as the United States, the law permits intelligence services to use "unvouchered accounts" (expenditures accounted for solely on the certification of a member of the executive branch, and not supported by a full set of receipts) in connection with some sensitive operations (e.g. foreign intelligence operations).[14]

4.3 FINANCIAL REPORTING

Public agencies, including intelligence services, are normally required by law to prepare detailed annual reports of their financial transactions.[15] Without such reports, external oversight bodies could not review service finances and activities.

Intelligence services normally deliver these reports to the executive, the SAI, and the parliament. As with intelligence budgets, however, these reports can vary in the amount of detail provided.

Just as the executive should be denied the power to determine unilaterally what budgetary information is disclosed and what may be withheld, it should also be denied the power to determine by itself what information is fit for inclusion in financial reports and what may remain secret. Instead, the parliament should create through legislation detailed criteria regulating what financial information must be made public and what can remain confidential (see Box 3).

As with intelligence budgets, Australia and France provide examples of good practice in this regard. Their intelligence services prepare relatively detailed financial reports for public disclosure. The publicly available reports of the Australian Security Intelligence Organisation (ASIO) contain subtotals for expenditure categories such as personnel, supplies (including goods and services), and depreciation/amortization costs. The reports also contain subtotals for income categories such as own-source revenue, assets sales, and government revenue.[16] French law requires that the financial reports of intelligence services include detailed annexes for each service mission. These annexes must include not only financial data but also an evaluation of the policy objectives and desired outcomes established at the start of the budget cycle.[17]

Box 3: Financial reporting under New Zealand law

This box distills selected provisions of the Public Finance Act of 1984 and the Security Intelligence Service Act of 1969, which jointly regulate the manner in which New Zealand's intelligence services prepare financial reports. It compares the requirements for intelligence services with those for other public bodies.

As soon as possible after the close of each fiscal year, public bodies in New Zealand (including the intelligence services) must prepare financial reports covering the prior fiscal year and deliver them to the responsible minister. The reports must include complete financial data as well as information on agency operations and a statement of agency performance. In general, the reports must provide enough information to enable an informed assessment of the agency's performance during the prior fiscal year—especially with regard to the objectives, indicators, and standards set out for the agency at the start of the year.

With regards to most public bodies, the law requires the responsible minister, once in receipt of the report, to present it to the parliament and then publish it as soon as possible. For intelligence services' reports, however, arrangements differ. Rather than submitting the full report to the plenary of the parliament, the responsible minister submits it only to the Intelligence and Security Committee of parliament, whose members are authorized to view classified information. For the plenary of the parliament, the minister prepares a redacted version, which must include a statement of total expenditures. It is this redacted version of the report that the minister later makes public.

For the same reasons cited above (see Section 3.3) with regard to budgetary information, intelligence services should make the public versions of their financial reports as detailed as possible without jeopardizing the confidentiality of their work or endangering national security.

5. PARLIAMENTARY OVERSIGHT

This section focuses on the oversight role played by parliament during the final three stages of the budget cycle—scrutiny and approval, implementation, and *ex post* review. Although the work of intelligence services involves sensitive matters, parliaments should subject intelligence service finances to the same level of scrutiny given to the finances of other public agencies. The only concession made should be the use of more circumspect oversight mechanisms.

Necessarily, most parliamentary oversight of intelligence services takes place behind closed doors. Yet it remains important that parliamentarians keep the public informed about the oversight work through public reports and public hearings (see Nathan—Tool 3). Transparency promotes public confidence not only in parliamentary oversight but also in the work of the intelligence services.

5.1 SCRUTINY AND APPROVAL OF BUDGETS

In most democratic countries, parliaments scrutinize, amend, and approve agency budgets

proposed by the executive. There is no valid reason why intelligence service budgets should be excluded from this process.

In order to protect classified information, parliaments may create special mechanisms to scrutinize classified sections of the budget. However, regardless of which mechanisms are used, the plenary should always vote on intelligence service appropriations as part of its approval of the government's budget. Plenary votes should be in addition to, and not a substitute for, full scrutiny by one or a combination of: a budget committee, intelligence oversight committee, or special confidential committee.[18]

5.1.1 Budget committees

Some parliaments use standard budget (or appropriations) committees to scrutinize the finances of the intelligence services. These committees may designate members, known as rapporteurs, to take responsibility for a particular service, ministry, or mission. Such rapporteurs normally produce reports containing recommendations on the basis of which the full committee discusses, amends, and approves the service budgets.

Budget committees are in many ways well placed to evaluate intelligence service budgets within the broad context of the entire executive budget. But in the absence of specialized rapporteurs, committee members will likely not have the necessary time or subject-specific expertise to properly scrutinize intelligence services' budgets. Budget committees also tend to lack sufficient access to classified information, further limiting their ability to scrutinize services' budgets.

5.1.2 Intelligence oversight committees

Intelligence oversight committees normally have access to classified information not available to other members of parliament (see Farson—Tool 2, and Nathan—Tool 3). They typically focus on *ex post* review of intelligence services' activities, including their finances. In some countries, however, their responsibilities extend to budgetary scrutiny and approval as well. In Hungary, the parliamentary National Security Committee scrutinizes and provides an opinion on the proposed budgets for the intelligence services. This includes scrutiny of the classified sections of the budget that are not made available to the plenary of parliament.[19] The US Congress's more complex process is described in Box 4. Elsewhere, (e.g., in Germany, see Box 5) intelligence oversight committees play a secondary role, advising other committees (such as budget or appropriations committees) that have primary responsibility for scrutinizing budgets.

Intelligence oversight committees are particularly well suited to examine and understand intelligence service budgets because of their familiarity with service activity, procedures, and policies. Yet the effectiveness of such scrutiny depends on several factors:

- the committee's resources, investigative powers, and access to classified information
- the degree to which committee members have the time, staff, and expertise to carry out their responsibilities
- the will of the committee members to carry out their responsibilities
- the committee's ability to influence the budgetary process (especially when its role is advisory)

Box 4: Congressional scrutiny and approval of US intelligence service budgets[20]

The process by which the US Congress scrutinizes and approves intelligence service budgets involves no fewer than eight committees and subcommittees. It has two distinct aspects: authorization and appropriation.

Authorization

Congressional authorization bills, when signed by the president, regulate the activities of government agencies, including their budgets. For intelligence service budgets, the authorization process begins with proposals submitted to Congress by the executive. The proposals are reviewed in the House of Representatives by the Permanent Select Committee on Intelligence and the Armed Services Committee, and in the Senate by the Select Intelligence Committee and the Armed Services Committee. These committees can reallocate amounts within the budgets; they can also prohibit particular activities and include new initiatives. Once a chamber's committees have finalized an authorization bill, it proceeds to the floor for a vote by the plenary. Once the House and Senate have both approved authorization bills, the bills are reconciled, approved again by each chamber, and sent to the president for his or her signature.

Each intelligence authorization bill has a classified annex that lists by category of activity the amounts each service is authorized to receive and the purposes to which the funds should be put. In this way, authorization bills (once signed into law) establish parameters for intelligence spending. However, authorization laws do not guarantee that authorized programmes will indeed be funded. Final funding decisions are made during the appropriation process.

Appropriation

Appropriation legislation is similar to budget legislation in other countries; it is the legal instrument that allocates treasury funds to an agency or programme. Both the House Appropriations Committee and the Senate Appropriations Committee have defense subcommittees with jurisdiction over the budget of nearly all of the US intelligence community. Based on proposals received from the executive, these subcommittees draft intelligence appropriation bills.

Although appropriation bills must conform generally to existing authorization legislation, they can increase or decrease funding for specific intelligence programmes. If no such legislation exists, appropriation bills can include blanket authorizations for all intelligence activity.

As with authorization legislation, appropriation bills must endure a complex approval process. They must be approved by the subcommittees, then the full committees, and then the plenary of each chamber—after which they have to be reconciled, approved again by each chamber, and finally sent to the president for his or her signature.

Under the right circumstances, intelligence oversight committees with significant budgetary responsibilities can use (in collaboration with other relevant committees) the power of approval to ensure that proposed budgets take into account previous committee recommendations on ways to improve service effectiveness, efficiency, and legal compliance.

5.1.3 Special confidential committees

Parliaments sometimes use a third mechanism, the special confidential committee, to scrutinize intelligence service budgets. A good example of this mechanism is the Confidential Committee created by the German Bundestag (see Box 5).

Box 5: The Confidential Committee of the German Bundestag[21]

The Bundestag, the lower house of the German parliament, refers budgetary matters involving the three federal intelligence services to a special Confidential Committee that it has created. This committee performs the same functions that the Bundestag's Budget and Public Audit Committees perform with regard to other public departments and agencies. That is, it scrutinizes and can amend budgets proposed by the executive, and reviews their implementation – this box focuses on the Committee's budgetary scrutiny and approval functions.

Selection of committee members

The Confidential Committee has ten members whose seats are allocated proportionally by political party in accordance with each party's representation in the Bundestag. Nominees do not require security clearance, but they must be elected by what is known as a "chancellor's majority," meaning that a majority of Bundestag members must vote for them, indicating that they have the trust of the parliament.

Scrutiny and approval of intelligence budgets

The committee's scrutiny and approval of intelligence service budgets proceeds as follows:

1. The executive provides the committee with a detailed budget for each intelligence service.
2. The committee meets with ministry officials and senior service management to discuss the proposed budgets.
3. The committee consults with the Bundestag's intelligence oversight committee.
4. The committee amends the budget as it sees fit before returning it to the executive, which must ordinarily accept the changes.
5. The committee chair communicates to the Budget Committee the total amounts allocated to each service. The Budget Committee then incorporates these figures (without debate) into its budget recommendations.
6. The plenary of the parliament votes on the full government budget.

Investigative powers and access to information

The law grants to the Confidential Committee strong investigative authority and broad access to classified information, including the ability to review all files and documents under the control of the intelligence services and to inspect all service premises. The committee can compel service officials and members of the executive to answer questions, and can commission external experts to assist with its work if necessary.

5.2 MONITORING IMPLEMENTATION OF BUDGETS

Once the budgets of public agencies are approved, parliaments have the responsibility to monitor agency expenditures to ensure that the budgets are being implemented properly. With regard to intelligence services, the monitoring is usually performed by the parliament's intelligence oversight committee (or a special confidential committee)

whose members have privileged access to classified information. In practice, however, intelligence oversight committees tend to request financial information only if allegations of misconduct have been raised about a particular programme or activity. This is because most parliamentarians have neither the time nor the resources to examine in detail large amounts of financial information throughout the year.

In view of these limitations, the implementation monitoring performed by the parliament usually relies on information disclosed proactively (that is, without being requested) by the executive and the intelligence services. Indeed, applicable law in many democratic countries requires the executive and/or the intelligence services to disclose information about service finances on a periodic basis.[22] In Italy, for example, the prime minister is required to report every six months to the Parliamentary Committee for the Security of the Republic (COPASIR) on the implementation of the intelligence service budgets.[23]

Parliaments also have to consider requests for additional funding that arise during the fiscal year. In the case of intelligence services, these requests may relate to unforeseen events, such as terrorist attacks. As with other implementation-related matters, consideration of these requests is typically delegated to the parliament's intelligence oversight committee. In Spain, for example, requests for additional funding are reviewed by the Secret Funds Committee, whose opinion informs the plenary vote.[24]

5.3 *EX POST* REVIEW OF FINANCES

The *ex post* review of public agency finances is primarily the responsibility of each agency's internal audit mechanisms (see Section 4) and the national SAI (see Section 6). Nevertheless, parliaments do play a role in this process, reviewing the work of the auditors and conducting their own investigations. At the conclusion of this process, some parliaments pass legislation to "discharge" the implementation of the budget (i.e., to officially approve government accounts for a given period).

5.3.1 Parliamentary mechanisms for ex post review

Parliamentary public accounts or public audit committees (PACs), which conduct *ex post* review of public bodies' finances, are not usually responsible for ex post review of intelligence service finances because of their sensitive nature. Instead, many parliaments make special arrangements for the review of intelligence service finances. In the United Kingdom, for instance, the National Audit Office's (the United Kingdom's SAI) reports and opinions on the intelligence services are only submitted to the chair of the Public Accounts Committee.[25] The primary responsibility for their review lies instead with the Intelligence and Security Committee, whose oversight mandate includes *ex post* review of intelligence service finances (see Box 6). Elsewhere, e.g., in Germany (see Box 5), parliaments have a dedicated committee for performing parliament's tasks with regard to budgets and accounts that contain classified information.

Box 6: The role of the UK Intelligence and Security Committee in *ex post* review

The UK parliament's Intelligence and Security Committee (ISC) includes members from both chambers. Its mandate is to oversee "policy, administration and expenditure" of the intelligence and security services.[26]

In accordance with this mandate, the ISC conducts *ex post* review of service finances, primarily on the basis of the annual audit opinions and reports prepared by the National Audit Office (NAO). As part of this process, the ISC holds hearings with NAO representatives and senior service management to discuss the NAO audit.

In its own annual report, the ISC includes an assessment of service finances.[27] Initially, the ISC submits its report to the prime minister, but the report is subsequently made public.[28] In addition, the ISC employs a staff investigator who can be assigned at any time to examine, among other things, aspects of service activity with important financial implications.[29]

5.3.2 The process and purpose of *ex post* review

Ex post parliamentary review of intelligence service finances normally focuses on the reports of SAIs. Parliamentarians responsible for *ex post* review also consider the annual reports and financial statements prepared by the intelligence services.[30] Hearings during which SAI auditors, executive officials, and intelligence service management give testimony are an important part of the process.

The primary purpose of *ex post* review is to determine whether the intelligence services have:[31]

- implemented their budgets as authorized by the parliament at the start of the budget cycle.
- spent and accounted for public funds in accordance with applicable laws and policies.
- performed effectively and efficiently.
- achieved the policy objectives established at the start of the budget cycle (if performance budgeting is being used).

At the conclusion of the review process, the parliamentarians conducting the review may issue a report containing recommendations for improvement of a service's financial practices and control mechanisms. In countries (e.g., France, Germany, and Hungary) where the law requires the full parliament to discharge the budget, such reports can influence the plenary vote.

Ex post review also informs parliamentary approval of future budgets. Indeed, parliamentarians can use their *ex ante* budgetary powers to compel acceptance by the executive and the intelligence services of *ex post* recommendations. This leverage works best when there are strong links between the *ex ante* approval of budgets and *ex post* review of their implementation. This may be best achieved by making a single parliamentary committee responsible for both functions with regard to the intelligence services (as is the case in Germany, see Box 5). Alternatively, coordination can be enhanced through joint committee meetings and other forms of information sharing between committees responsible for *ex ante* scrutiny of the budget and those responsible for *ex post* review.

5.3.3 Requesting reports from SAIs

In some countries (such as France and the United States), the parliament can instruct the SAI to investigate a particular programme or expenditure or assess the value for money provided by a particular investment.[32] Empowering the parliament in this way can help to ensure that the work of the SAI supports the work of the parliamentary oversight committees. On the other hand, it can also overburden the SAI and politicize its work (if, for example, influential parliamentarians instruct the SAI to investigate an issue for partisan reasons). In France, therefore, the law limits the number of requests that the parliament can make and leaves open the possibility that the Court of Audit may decline one or more of the requests. Similarly, German law permits the parliament to request an investigation by the Federal Court of Audit (FCA) but denies the parliament the power to compel FCA investigations, thus preserving the FCA's independence.[33]

6. SUPREME AUDIT INSTITUTIONS

In every democratic country, there exists some form of autonomous SAI responsible for auditing public agencies, including the intelligence services. Although SAIs focus primarily on the financial aspects of government activity, their audits may extend to other aspects of government service. A full discussion of the different types of SAIs is beyond the scope of this tool, but it can be noted briefly that SAIs fall into two broad categories: the "court" model (such as the French Court of Audit) and the "office" model (such as the UK National Audit Office and the US Government Accountability Office). Regardless of their specific form, SAIs are usually the main external body responsible for *ex post* review of intelligence service finances. The points made in this section apply to both types of SAIs.

6.1 INDEPENDENCE

In order for SAIs to perform their functions effectively, they need to be fully independent from the executive and all entities that they audit. In fact, the UN General Assembly has passed a resolution recognizing the importance of SAI independence.[34] Specifically, SAIs require:

- *Organizational independence*
  SAIs should be established by law as autonomous institutions with their own budgets.
- *Operational independence*
  SAIs should be free to determine what they audit, how and when they audit, as well as what findings and recommendations they draw from such audits. Auditors' work must be safeguarded from interference by any other body.
- *Personal independence*
  Personal independence refers to the position of auditors themselves. Senior officials of SAIs should be appointed in a way that promotes the selection of persons who have appropriate expertise and are independent of any affiliations or interests that could compromise their position as an auditor. This demands a transparent, inclusive, and merit-based process that requires candidates to receive the support of both the parliament and the executive. Once appointed, auditors should have their independence guaranteed by law through fixed tenures and other measures that protect them from retaliation should their findings prove unfavourable to the incumbent executive. Finally, senior auditors should avoid political or business

activities that could compromise their independence and/or be perceived as conflicts of interest.

6.2 FUNCTIONS

The primary functions of an SAI are:

- revealing problems with legality, efficiency, effectiveness in financial management, as well as other deviations from accepted standards
- making recommendations for the improvement of financial management—including internal controls, risk management, and accounting systems
- assuring the parliament of the accuracy and regularity of government accounts, thereby helping to ensure that the executive complies with the will of the parliament
- assuring the public that its money is being spent lawfully, appropriately, efficiently, and effectively
- holding public agencies to account for their use of public money

While many of these functions are *ex post*—they entail the review of financial activities after they have taken place—SAIs may also play an *ex ante* role. Notably, an SAI (such as the German Federal Court of Audit, see Box 7) may be mandated to provide opinions on draft budgets.[35] This can be seen as a preventative function aimed at identifying and remedying financial problems before they occur. For example, an SAI might recommend the allocation of additional funding to a particular activity or type of expenditure if its previous audits have consistently identified over-spending on such matters.

It is not the responsibility of the SAI to search out cases of fraud or corruption; but should evidence of such practices be discovered, the SAI should report them to appropriate members of the executive and/or appropriate law enforcement agencies.

6.3 AUDITING INTELLIGENCE SERVICES

SAIs should conduct intelligence service audits using the same standards that they apply to audits of other public agencies, and SAI jurisdiction should extend to all aspects of intelligence service finances. The executive should not be permitted to exempt any area of intelligence activity from external financial oversight, because this both undermines the independence of the SAI and increases the risk that illegal or inappropriate uses of money may be covered up.[36]

Some countries (such as France and the United States) exempt certain operational accounts of intelligence services from SAI audit. In such cases, good practice requires that another independent body be designated to audit the exempted accounts. In France, exempted accounts are audited by the Special Funds Committee, a hybrid group of parliamentarians and auditors.[37] In the United States, exempted, "unvouchered accounts" (expenditures accounted for solely on the certification of a member of the executive branch) cannot be examined by the Government Accountability Office (GAO) but may be audited by congressional intelligence oversight committees.[38]

Regardless of how the review is performed, all intelligence service financial activity should be subject to audit by a body external to both the intelligence community and the executive. In general, SAIs are the bodies best suited to perform this auditing.

Box 7: Germany's Federal Court of Audit

The German Federal Court of Audit (FCA) is tasked with auditing all federal government bodies, including the federal intelligence services.[52]

Functions

The functions of the FCA with regard to federal government bodies include:

- auditing their income, expenditures, assets, and liabilities and examining any actions they have taken that may have financial consequences
- supporting the parliament in the exercise of its right to set agency budgets, including by providing opinions on draft budgets.
- supporting the parliament in deciding whether to grant discharge to the executive with respect to the executive's management of public funds[53]

Scope of Audits

Governing law places no restrictions on FCA activity. Consequently, the FCA alone decides which agencies it will audit and when and how the audits will take place. Parliament—in this context the Confidential Committee of the Bundestag—can request FCA audits, but it cannot compel the FCA to act. FCA audits determine whether agencies have observed the laws and regulations governing financial activity. In particular, they determine whether:

- provisions of the budget law have been observed.
- the agency's income, expenditure, asset, and liability records are orderly and properly substantiated with documents.
- public funds have been administered efficiently.
- assigned tasks have been completed effectively.

Intelligence issues raised by the FCA are addressed by the Confidential Committee (see Box 5), as part of the budget discharge process and in subsequent budget discussions. Accordingly, SAI representatives often take part in Confidential Committee meetings, creating a useful link between the audit and appropriation processes.[54]

Composition

The FCA is led by a president and a vice president. Both are nominated by the executive and elected by the parliament. Each can serve a maximum term of twelve years. The FCA is divided into thematic divisions, each headed by a director and his or her deputy. All of these people are "members of the court," meaning that they enjoy judicial independence. Most audit-related decisions are made by "colleges" of two members of the court (the relevant director and section head); where there is disagreement, the president joins them to form a college of three.[55]

Access to Information

The law obligates all government agencies, including the intelligence services, to provide the FCA with any document it deems necessary to the completion of its work. There are no limitations on this obligation.[56]

Reports

While the FCA ordinarily makes its reports public, its reports on the intelligence services are not made public. Instead they are delivered to the Confidential Committee, the Bundestag's intelligence oversight committee, and relevant executive bodies.[57]

6.4 TYPES OF AUDITS

The types of audits performed by SAIs vary from country to country, but the following three types are nearly universal:

- *Financial audits*
  These determine the accuracy and fairness of the financial statements prepared by public agencies.
- *Compliance audits*
  These determine whether the income and expenditures of an agency comply with applicable laws and regulations, including annual budget laws.
- *Performance or value-for-money (VFM) audits*
  These determine whether agencies have been effective and efficient in fulfilling their mandates and objectives—that is, whether taxpayers have received value for the public funds invested in the agency.

With regard to intelligence services, SAIs primarily conduct financial and compliance audits focusing on internal financial controls, risk management, and accounting systems.

Because SAIs cannot review each and every financial transaction made by an agency, most use a risk-based approach to assess the validity of their findings. Specifically, they evaluate the risk that the financial statements being presented to them are inaccurate. They do this by assessing, inter alia, an agency's accounting and reporting procedures, weaknesses in its internal controls, and weaknesses in the SAI's own detection procedures.

Performance auditing of intelligence services can be very challenging because of the reasons discussed in Section 2 of this tool, especially the uncertainty of outcomes and intangibility of benefits that characterize intelligence work. SAIs may find it difficult, for instance, to assess the value of operational activities (such as agent running and surveillance) whose success or failure can be difficult to quantify. As a result, some SAIs refrain from evaluating performance in these areas.

Performance audits can however, produce findings that financial and compliance audits cannot. Consider, for example, the case of a major capital project or large-scale procurement programme that passes financial and compliance muster because it has been accounted for properly and complies with all applicable laws and regulations. It may nevertheless represent poor value for the money spent—a failing that may be revealed only by a performance audit.

To the extent that SAIs conduct performance audits of intelligence services, they usually focus on specific issues or themes across multiple agencies (see Box 8)—such as information technology systems or security clearance procedures.

Box 8: Performance auditing in Canada

In 2004, the Auditor General (AG) of Canada conducted a performance audit of the Canadian Security Intelligence Service and other intelligence-related agencies. This audit examined "the overall management of the Public Security and Anti-Terrorism initiative [and] the co-ordination of intelligence among departments and agencies and their ability to provide adequate information to enforcement personnel."[39] It took place in the wake of significant antiterrorism investments made by the Canadian government following 9/11.

In the final audit report, the AG concluded, among other things, that "the government did not have a management framework that would guide investment, management, and development decisions and allow it to direct complementary actions in separate agencies."[40] Furthermore, according to the AG, "the government as a whole failed to achieve improvements in the ability of security information systems to communicate with each other."[41] More generally, the AG found that there were "deficiencies in the way intelligence is managed across the government."[42]

6.5 ACCESS TO INFORMATION

SAIs need unrestricted access to information, both as a prerequisite for high-quality audits and as a guarantor of operational independence. An intelligence service's understandable desire to protect confidential information from unauthorized disclosure does not diminish the SAI's need. Accordingly, it is good practice for the law to grant SAIs access to *all* documents, persons, and physical locations that auditors deem to necessary for their work. This is, for instance, the case in South Africa (see Box 9), as well as in Germany (see Box 7), where such access includes information about ongoing intelligence operations. It is essential but not sufficient for access to be enshrined in the law(s) regulating the SAI. Lawmakers must also ensure that laws on intelligence services and classified information do not contradict such provisions on SAIs' access. The law should also grant SAIs powers designed to support their access to information. Such powers may include the power of subpoena, the power of search and seizure, and the power to compel testimony under oath or affirmation (see Box 9).

In some states, the law places restrictions on SAI access to information. This is true of the UK National Audit Office, for example, which has restricted access to information concerning intelligence sources and methods. This restriction is narrow and clearly defined, and is not thought to hinder the NAO's work. Elsewhere, however, restrictions on SAI access to information are much broader. In the US, for example, the law affords the intelligence community considerable discretion to decide what information it will share with the Government Accountability Office, on a case-by-case basis.[45] Furthermore, the GAO is barred from accessing information relating to "unvouchered accounts" sources, methods, and covert actions.[46] Limitations on access to information hinder the work of the GAO and its counterparts in other states; they can serve to reduce the effectiveness and comprehensiveness of independent financial oversight.

Even when the law grants SAIs full access and strong enforcement powers, these powers may not be sufficient to ensure access to all the information that an SAI deems relevant. Because of the confidential nature of many intelligence-related matters, SAIs face significant practical obstacles in accessing certain types of information. Notably,

they would have difficulty interviewing paid informants, obtaining information on covert operations, and verifying the existence of assets used by confidential agents.

Box 9: Powers of the South African auditor general[43]

The auditor general (AG) of South Africa has strong powers that he or she can use to gain access to needed information. This box summarizes those powers. It should be noted, however, that in practice the inclusion of such powers in the AG's legal framework does not necessarily ensure the disclosure of relevant information by secretive intelligence services.[44]

Access to information

The law grants the AG, when performing an audit, full and unrestricted access at all reasonable times to:

- any document, written or electronic record, or other piece of information possessed by the auditee that elucidates the business, financial activity, financial position, or performance of the auditee
- any asset of, or under the control of, the auditee
- any representative of the auditee or member of its staff

Audit powers

When performing an audit, the AG may:

- direct a person to disclose under oath or affirmation, either orally or in writing, information that may be relevant to the audit—including confidential, secret, or classified information.
- question any person about such information.

Additionally, when performing an audit, the AG may obtain from a judge or magistrate a warrant to:

- enter any property, premises, or vehicle on reasonable suspicion that relevant information is being kept or hidden therein.
- search any property, premises, or vehicle as well as any person on the premises or in the vehicle for potentially relevant information.
- seize any potentially relevant information for the purpose of completing the audit.

In general, the AG's right to access needed information overrides the obligations of the intelligence services to maintain confidentiality. For example, a person who is ordinarily prohibited from disclosing information relating to an intelligence matter may nevertheless be required to disclose that information to the AG. In such cases, complying with the AG's request is not considered a breach of the person's non-disclosure obligation.

The impact on audits of legal and practical limitations on access to information depends, inter alia, on the type of audit being conducted and the readiness of the intelligence service to cooperate. Under some circumstances, limits on access to information can meaningfully impair an SAI's ability to perform its work, undermining the integrity of the audit process and resulting in a lower-than-desired level of audit assurance. Indeed, it is particularly problematic if auditors are unaware that information, which may have altered their conclusions, has been withheld from them. In the absence of such information, they may even issue unqualified opinions that give a false sense of assurance and accountability.

Problems of this sort are most likely to arise in countries where the authority and independence of the SAI has not been fully established and/or the SAI has an adversarial relationship with the intelligence services being audited. Should an SAI determine that restrictions on its access to information have impaired its ability to issue an accurate audit opinion, international auditing standards require the SAI to issue a qualified opinion. Upholding this professional duty ensures that any legal or practical limitations on access to information are factored into audit opinions and reports.

6.6 PROTECTION OF INFORMATION

In order to assure both the intelligence services and the executive that information disclosed to auditors will remain confidential, many SAIs have established special units with secure facilities and security-cleared staffs to perform intelligence audits. (As a general rule, SAI personnel auditing intelligence service records should be held to the same security standards as service personnel with access to the same records—including a legal obligation to protect the secrecy of classified and other confidential information.[47]) Handling confidential information in a professional manner builds trust between SAIs and the intelligence services and increases the likelihood that information will be readily provided in the future.

6.7 REPORTS

Reports are the primary means by which auditors communicate their findings and recommendations. The recipients of audit reports include intelligence service management, executive officials, parliamentarians, and members of the general public. Often, these stakeholders take action based primarily on SAI reports. Most significantly, parliamentarians use SAI reports as the basis for their oversight of intelligence service finances. Indeed, it is primarily through parliamentary decisions on future budgets that SAIs' findings and recommendations can have an impact upon intelligence services and the executive.

6.7.1 Secrecy

Because SAI reports on intelligence services contain references to classified information, unredacted versions are usually withheld from the public and even from most members of parliament. The law and/or customary practice typically limits receipt of the full (classified) reports to senior service management, senior executive officials, members of parliamentary oversight committees, and, in some cases, members of parliamentary finance/budget committees.

Although sensitive national security information contained in SAI reports should certainly remain within the "ring of secrecy," there are many portions of these reports that can and should be made public. In this regard, the Auditor General of South Africa has stated that his reports on the intelligence services should be made public because there is nothing in them that, if disclosed, would prejudice the services or compromise the security of the country.[48]

Blanket bans on the publication of intelligence service audits and routine classification of their contents are inconsistent with the basic democratic principles of transparency, open government, and freedom of information. With respect to this issue, the South African

constitution is particularly progressive, requiring the disclosure of all reports prepared by the Auditor General, including those relating to the intelligence services, subject to the removal of sensitive information.[49] In general, classification should be the exception to the general rule of publication, permitted only when necessary to protect legitimate national security interests.

In no event should members of the intelligence services or the executive be able to use secrecy provisions to conceal the unlawful use of public funds. It is good practice for the law to contain an override explicitly allowing the disclosure of classified information when doing so is necessary to reveal wrongdoing. This language from the South African Public Audit Act describes such an override:

> *(1) The Auditor-General must take precautionary steps to guard against the disclosure of secret or classified information.*
>
> *(2) Steps taken in terms of subsection (1) may not prevent the disclosure of any audit finding by the Auditor-General or an authorised auditor on any unauthorised expenditure, irregular expenditure or fruitless and wasteful expenditure…or on any other irregular or criminal conduct relating to the financial affairs of an auditee, but any such disclosure may not include facts the disclosure of which would harm the national interest.*[50]

6.7.2 Making information public

SAIs should, at a minimum, make public the following types of information about their audits/reviews of intelligence services:

- *A list of the audits that the SAI has performed or will perform*
  Each reference can be as simple as a title and brief explanation.[51]
- *The basic audit opinion on the service's financial statements*
  Normally a very short document, the basic opinion discloses little information but confirms that an interaction with the service has occurred.
- *Public versions of classified reports*
  SAIs should issue public versions of their reports, including periodic and performance audits that address intelligence services (see Box 8, for example). This may be done by redacting (removing) sensitive information from classified versions of reports, producing a separate public version of reports, or by including all classified information in annexes that are not made public. While most parliamentary and expert oversight bodies issue public versions of their reports, this practice has not yet become widespread among SAIs.

6.8 IMPORTANCE OF TRANSPARENCY IN THE WORK OF SAIS

In keeping with the principles of democratic governance, the public needs to know as much as possible—subject to the confidentiality limitations discussed previously—about the work of SAIs and their reports on the intelligence services. Informing the public about SAI audits of intelligence services helps generate confidence in and support for both the audited service and the SAI. Assuring the public that the intelligence community is being subject to proper scrutiny contributes to the helpful perception that the intelligence services are acting professionally, using public funds appropriately, and operating within the limits of the law.

Moreover, transparency helps to dispel myths about the intelligence services—concerning, in particular, their use of public funds. This is particularly necessary in countries in which levels of trust in intelligence services remain low and services have previously misused funds. It also serves to generate and inform public debate on the proper role of the intelligence services. This can be important when governments face large budget deficits and have to cut public services.

7. RECOMMENDATIONS

Although there is no single "best" approach to the oversight of intelligence service finances, the following recommendations, distilled from the laws, institutional models, and practices discussed in this tool, are good practices that can be adapted to fit many different legal and institutional models. Most of these recommendations assume that legal and institutional frameworks for budgeting and auditing already exist and that a legal framework for the management and use of public funds is already established.

Recommendations relating to budgeting and financial reporting

- Intelligence service budgets should be "comprehensive," meaning that they should encompass all of a service's financial activity. The law should specifically prohibit services from engaging in financial activity not included in their budgets.
- Governments should disclose as much as possible about intelligence service budgets without jeopardizing public safety or national security. At a minimum, they should disclose the total amount being allocated to a service, the subtotals for particular categories of costs, and the objectives associated with particular expenditures. Budgetary information should be classified only when secrecy is strictly necessary to protect legitimate national security interests.
- Parliaments should enact legislation to govern what financial information (including budgets and financial statements) must be disclosed and what may remain confidential and/or subject to extraordinary accounting and auditing procedures.
- Intelligence services should prepare public versions of their financial statements containing as much information as possible.

Recommendations relating to internal financial controls

- Intelligence services should not be exempt from laws regulating the internal financial controls and audit mechanisms of public agencies.
- If an intelligence service is to be permitted occasional deviations from the laws and regulations governing the management and use of public funds, the authority to permit such deviations should be grounded in legislation.

Recommendations relating to external financial oversight

- The law should require SAIs to audit the finances of intelligence services to determine whether service financial statements are accurate and fair, whether service financial transactions comply with applicable laws and regulations, and whether public funds

have been used effectively in a manner that provides value for money. In pursuit of these objectives, SAIs should be empowered to audit all aspects of service activity, including special accounts relating to covert or otherwise sensitive operations.

- Parliaments and SAIs should subject intelligence service finances to the same level of scrutiny applied to the finances of other public agencies. This scrutiny should take place throughout the budget cycle, beginning with full examination of the classified sections of budget proposals and concluding with *ex post* review and auditing of service financial records.
- The law should grant external oversight bodies access to all information they deem necessary for the completion of their work, whether that information is held by the intelligence service being audited or by another public body. Such access should be supported by appropriate investigative powers sufficient to compel disclosure.
- Parliaments and SAIs with access to confidential information should take steps to protect that information from unauthorized disclosure. Such measures should ensure that the information is made available only to personnel with a need to know it, that it is physically and technologically secure, and that sanctions exist to deter unauthorized disclosure.
- Members of parliamentary committees responsible for financial oversight should have sufficient human and technological resources to enable them to understand intelligence service finances and conduct meaningful scrutiny.
- Parliaments should ensure that SAIs have the authority and resources necessary to complete their work. Furthermore, they should promote the implementation of SAI recommendations by the intelligence services.
- Parliaments should ensure that proper links exist among external oversight bodies so that the results of *ex post* reviews and audits can be used to inform the scrutiny of budget proposals in subsequent years.
- Parliamentary committees responsible for financial oversight of intelligence services should actively engage with SAIs. This should include: reviewing their reports, holding follow-up meetings, and taking steps to ensure SAIs have the adequate powers and resources to audit to intelligence services.
- Parliaments and SAIs have a responsibility to keep the public informed about their oversight of intelligence services. They should prepare public versions of their findings and make periodic reports to the public on their activities.

Endnotes

1. This tool draws upon the proceedings of and written submissions to a DCAF workshop on the financial oversight of intelligence services. Participants included senior members of supreme audit institutions, a representative of a national parliament, former intelligence officials, and academics from a range of countries. All proceedings were off the record and have therefore not been cited directly. The participants also provided helpful feedback on a draft of this tool. The author would like to express his gratitude to all members of this group and also thanks his DCAF colleagues Hans Born, Benjamin S. Buckland, and Gabriel Geisler Mesevage for their invaluable comments on earlier drafts.
2. "Value for money" refers to the economy, efficiency, and effectiveness with which an organization uses its resources in carrying out its responsibilities; see "Performance Audit" in: International Organization of Supreme Audit Institutions, Financial Audit Guideline – Glossary of Terms to the INTOSAI Financial Audit Guidelines.
3. United States, Central Intelligence Agency; appropriations; expenditures, U.S. Code 50 §403j (available at http://us-code.vlex.com/vid/central-intelligence-agency-expenditures-19266900).
4. For examples of such exceptions, see United Kingdom, The Defence and Security Public Contracts Regulations 2011, No. 1848, Section 7 (available at http://www.legislation.gov.uk/uksi/2011/1848/made).
5. Auditor General of Canada, *Report of the Auditor General of Canada* (1996), "Chapter 27—The Canadian Intelligence Community—Control and Accountability," Section 27.107 (available at http://www.oag-bvg.gc.ca/internet/English/parl_oag_199611_27_e_5058.html).
6. For more detailed information, see David Johnston and Mark Mazzetti, "A Window Into C.I.A.'s Embrace of Secret Jails," *New York Times*, August 12, 2009; David Johnston, "Ex-C.I.A. Official Admits Corruption," *New York Times*, September 29, 2008; Matthew Barakat, "Feds: Misconduct by CIA's Foggo spanned decades," *Associated Press*, February 25, 2009; and U.S. v. *Foggo and Wilkes*, U.S. District Court of Southern California, Grand Jury Indictment, June 2005.
7. The World Bank, *Public Expenditure Management Handbook* (Washington: The World Bank, 1998), "Code of Practices on Fiscal Transparency," Annex J.
8. Todor Tagarev, (ed.), *Building Transparency and Reducing Corruption in Defence: A Compendium of Best Practices* (Geneva: NATO/DCAF, 2010), p. 64. For an example from national law, see South African Public Finance Management Act, No. 1 of 1999, Section 38(2).
9. For a more detailed discussion of different approaches to budgeting see The World Bank, *Public Expenditure Management Handbook*, pp. 12–16; Tagarev, *Building Transparency*, p. 59; and Organisation for Economic Co-operation and Development (OECD), "Performance Budgeting: A User's Guide," Policy Brief (March 2008).
10. The UK Single Intelligence Account aggregates the budgets of the three civilian intelligence services.
11. For a more detailed discussion, see Nicolas Masson and Lena Andersson, *Guidebook: Strengthening Financial Oversight in the Security Sector* (Geneva: DCAF, 2012).
12. France, Mission Ministérielle Projets Annuels de Performances, "Annexe au projet de loi de finance pour Défense" (2010), pp. 36–37.
13. On the importance of decision makers having access to all budgetary information, see: The World Bank, *Public Expenditure Management Handbook*, pp. 1–2.
14. United States General Accounting Office (GAO), "Central Intelligence Agency: Observations on GAO Access to Information on CIA Programs and Activities," GAO-01-975T (July 2001), p. 10; and United States, Central Intelligence Agency; appropriations; expenditures, U.S. Code 50 §403j.
15. See for example, Australia, Financial Management and Accountability Act 1997, Section 49.
16. Australian Security Intelligence Organisation, Financial Statements, in *Annual Report 2010–11* (Canberra: 2011), pp. 133–151 (available at http://www.asio.gov.au/img/files/Report-to-Parliament-2010-11.pdf).
17. France, Loi organique n°2001–692 du 1 août 2001 relative aux lois de finances (LOLF), Article 54.
18. For a discussion of the Italian model in which the parliament votes on an aggregate amount, leaving the specific allocation of funds to the discretion of the executive, see Federico Fabbrini and Tomasso Giupponi, "Parliamentary and Specialised Oversight of Security and Intelligence Agencies in Italy," in *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, Aidan Wills and Mathias Vermeulen (Brussels: European Parliament, 2011), Annex A, p. 245.
19. Hungary, Act CXXV of 1995 on the National Security Services, Article 14(g).
20. Richard Best, *The Intelligence Appropriations Process: Issues for Congress* (Washington: Congressional Research Service, October 27, 2011); see also Richard Best and Elizabeth Bazan, *Intelligence Spending: Public Disclosure Issues*

(Washington: Congressional Research Service, February 15, 2007), p. 5; Frederick Kaiser, Walter Oleszeck, and Todd Tatelman, *Congressional Oversight Manual, Congressional Research Service* (Washington: Congressional Research Service, June 2011), pp. 16–19; Eric Rosenbach and Aki Peritz, *Confrontation or Collaboration? Congress and the Intelligence Community* (Cambridge, MA: Harvard, 2009), pp. 24–28; and James Saturno, *The Congressional Budget Process: A Brief Overview* (Washington: Congressional Research Service, 2004).

21. German Federal Budget Code, Article 10(a). See also Hans De With and Erhard Kathmann, "Parliamentary and Specialised Oversight of Security and Intelligence Agencies in Germany," in *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, Wills and Vermeulen, Annex A, pp. 225–226.
22. For a more detailed discussion, see Wills and Vermeulen, pp. 129–131.
23. Italy, Law 124/2007, Articles 33(8) and 29(2).
24. Spain, Ley 11/1995, Article, 2.2. See also Susana Sanchez Ferro, "Parliamentary and Specialised Oversight of Security and Intelligence Agencies in Spain," in *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, Wills and Vermeulen, Annex A, p. 271.
25. The chair of the Public Accounts Committee is always a member of the opposition.
26. United Kingdom, Intelligence Services Act 1994, Section 10 (1).
27. See for example, United Kingdom, Intelligence and Security Committee, *Annual Report 2010–2011*, CM 8114 (2011), pp. 12–16.
28. Ian Leigh, "Parliamentary and Specialised Oversight of Security and Intelligence Agencies in the United Kingdom," in *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, Wills and Vermeulen, Annex A, p. 298.
29. Ibid., p. 297; examples of the Investigator's work are discussed in United Kingdom, Intelligence and Security Committee, *Annual Report 2010–2011*, pp. 7, 16, 17, and 79.
30. OECD, "Relations Between Supreme Audit Institutions and Parliamentary Committees," Sigma Papers, No. 33 (Paris: OECD Publishing, January 2002), pp. 19–20.
31. In some countries, parliamentary *ex post* review also determines whether the SAI performed its audits in an appropriate manner.
32. France, Ministry of Budget, Public Accounts and Civil Service, "Guide to the Constitutional Bylaw on Budget Acts" (2008) p. 32; France, LOLF, Article 54 and Article 58; United States, Government Accountability Office web site (available at http://www.gao.gov/about/index.html).
33. German Federal Ministry of Finance, "The Budget System of the Federal Republic of Germany" (Berlin: 2008) p. 47.
34. UN General Assembly Resolution, "Promoting the efficiency, accountability, effectiveness and transparency of public administration by strengthening supreme audit institutions," United Nations Document A/RES/66/209 (15 March 2012),.
35. Ibid., p. 18.
36. This remains the case in the US, where the GAO's authority to audit several areas of the CIA's work are restricted both in practice and in law. See Intelligence Community Directive, No. 114, June 30, 2011; Gene Dorado (US Comptroller General), Letter to Director of National Intelligence James Clapper regarding "GAO Comments on Intelligence Community Directive Number 114: Comptroller General Access to Intelligence Community Information," 28 April 2011; and US GAO, "Central Intelligence Agency: Observations on GAO Access to Information on CIA Programs and Activities," GAO-01-975T (July 2001), pp. 4–8.
37. France, Loi n° 2001–1275 du 28 décembre 2001 de finances pour 2002, Article 154; France, L'Assemblée Nationale, "Rapport fait au nom de la Commission des Finances, de l'économie générale et du contrôle budgétaire sur le projet de loi de finances pour 2012: Annexe n° 12, direction de l'action du gouvernement publications officielles et information administrative" (14 October 2009), pp. 25–27.
38. United States, Auditing Expenditures Approved Without Vouchers, U.S. Code 31 §3524.
39. Office of the Auditor General of Canada, *March 2004 Report of the Auditor General of Canada* (2004), Section 3.2.
40. Ibid., Section 3.3.
41. Ibid., Section 3.4.
42. Ibid., Section 3.5.
43. South Africa, Public Audit Act, No. 25 of 2004, Sections 15–16.
44. South Africa, Ministerial Review Commission on Intelligence, *Intelligence in a Constitutional Democracy: Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP* (10 September 2008), pp. 226–227.
45. Intelligence Community Directive, No. 114; and Gene Dorado, Letter to Director of National Intelligence James Clapper, 28 April 2011.

46. United States GAO, "Central Intelligence Agency: Observations on GAO Access to Information on CIA Programs and Activities," pp. 4–8; Intelligence Community Directive, No. 114; and Frederick M. Kaiser, "GAO Versus the CIA: Uphill Battles against an Overpowering Force," *International Journal of Intelligence and Counterintelligence* Vol. 15, No. 3 (Fall 2002): pp. 345–353.
47. See, for example, Australian Auditor General Act 1997, Section 36; 31 U.S.C. 716; and OECD, "The audit of secret and politically sensitive subjects, comparative audit practices," Sigma Papers, No. 6 (Paris: OECD Publishing, 1996), p. 12.
48. South Africa, Ministerial Review Commission on Intelligence, *Intelligence in a Constitutional Democracy* (10 September 2008), p. 229.
49. Constitution of the Republic of South Africa, No. 108, 1996, Article 188(3).
50. South Africa, Public Audit Act, Section 18.
51. The Australian National Audit Office follows this practice. An example of an NAO audit plan can be found at http://www.anao.gov.au/~/media/Files/Audit%20Work%20Programs/2011_Audit_Work_Plan.PDF. An example of a NAO audit-in-progress outline can be found at http://www.anao.gov.au/Publications/Audits-in-Progress.
52. German Basic Law, Article 114(2); Germany, Federal Budget Code of 19 August 1969, *Federal Law Gazette I*, p. 1284, as most recently amended by Article 4 of the Act of 31 July 2009, *Federal Law Gazette I*, p. 2580, Section 10a (3); Section 88.
53. German Basic Law, Article 114(2); Audit Rules of the Bundesrechnungshof (Germany's Federal Court of Audit), last amended by Senate decisions on 29/30 August 2005, Articles 3, 56–57.
54. Germany, Federal Budget Code, Section 10a (3) and Sections 89–90; Audit Rules of the Bundesrechnungshof, Articles 4–5; The Budget System of the Federal Republic of Germany, pp. 49 and 51.
55. German Federal Court of Audit Act of 11 July 1985 (BGBl. I 1985, p. 1445) as last amended by article 17, Act of 9 July 2001 (BGBI. I, p. 1510), Sections 3, 5, 6, 9 and 19.
56. Germany, Federal Budget Code, Sections 10a (3) and 95.
57. Germany, Federal Budget Code, Section 10a (3); Audit Rules of the Bundesrechnungshof, Article 50.

TOOL 9

Handling Complaints about Intelligence Services

Craig Forcese

NINE

9

Handling Complaints about Intelligence Services

Craig Forcese

1. INTRODUCTION

This tool focuses on the role that oversight bodies play in handling complaints about intelligence services from the public, as well as complaints raised by members of the intelligence services. The need for a complaint-handling system is particularly acute for intelligence services because they are "often trusted with exceptional powers, such as surveillance or security clearance, which, if used incorrectly or mistakenly, carry the risk of serious injustice to individuals."[1] However, the justification for a complaint-handling system goes well beyond remedies for rights breaches. Complaint-handling mechanisms for intelligence services "can also bolster accountability by highlighting administrative failings and lessons to be learned, leading to improved performance."[2]

For these and other reasons, complaint-handling systems are considered to be an essential part of intelligence governance. In this respect, the UN special rapporteur's compilation of "good practices" on intelligence services and their oversight[3] urges the existence of procedures for bringing a "complaint to a court or oversight institution, such as an ombudsman, human rights commissioner or national human rights institution" whenever a person believes that his or her rights have been violated. Moreover, victims of illegal actions should "have recourse to an institution that can provide an effective remedy, including full reparation for the harm suffered."[4] This right to redress for human rights violations is grounded in international human rights law, which also requires that persons

have the right to an "effective remedy."[5] It is notable that "effective remedy" in this context should be construed as more than simply recompense for an established rights violation. It also includes a right to recourse to an institution able to adjudge whether a right has, in fact, been violated.[6]

The special rapporteur's report further urges that the institutions competent to address complaints and claims for remedies should be independent of the intelligence service and the political executive and "have full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders."[7]

It is these latter, design issues that raise the most complex challenges. There is now a fairly rich body of comparative data concerning the design and scope of complaint-handling bodies in the intelligence sector. While it is impossible with the resources available for this project to evaluate the actual workings of these entities, certain conclusions can be drawn from these systems' structure, scope, and powers. It is apparent from this review that while the need for complaint-handling systems is acute, designing an effective system may be more of an art than a science. States must decide whether to rely on conventional courts or design special complaint-handling bodies. In opting for the latter, states may be able to design special information-handling regimes that deal with the unique problems of secrecy and security raised by intelligence-related complaints. At the same time, recourse to specialized complaint-handling bodies raises other design issues; not least, questions of jurisdiction, membership, and powers to award remedies.

This tool examines these issues by subdividing its discussion into several different sections: bringing complaints; venues for complaints; complaints procedure and control of information; and remedies for complaints.

2. BRINGING COMPLAINTS

Standing rules determine who is competent to bring complaints. Complaints concerning intelligence services can be divided into two categories: first, "insider" complaints; and, second, "public" complaints. For the purposes of this tool, "insider" complaints are complaints brought to an independent body by intelligence or other government employees aggrieved by some action of the intelligence service. "Public" complaints are complaints brought by members of the public who are unconnected to the intelligence community or government.

2.1 INSIDER COMPLAINTS

In some jurisdictions, intelligence service or other government employees may bring grievances against an intelligence service. These insider complaints are sometimes tied to the intelligence service's treatment of the complainant. For instance, in Canada, the Canadian Security Intelligence Service (CSIS) performs almost all of the Canadian government's security screening investigations for the purpose of providing government employees with security clearances. An employee dissatisfied with the outcome of the clearance process may complain to an independent administrative body (or expert oversight body) known as the Security Intelligence Review Committee (SIRC).[8]

In other cases, "insider" complaints may be more general and amount to reporting intelligence service wrongdoing or excess. In Belgium, for example, the investigation service of the Standing Intelligence Agencies Review Committee (commonly known as Committee I) is empowered to:

> *[E]xamine the complaints and denunciations of individuals who have been directly concerned by the intervention of an intelligence service… Any public officer, any person performing a public function, and any member of the armed forces directly concerned by the directives, decisions or rules applicable to them, as well as by the methods or actions, may lodge a complaint … without having to request authorisation from his superiors.*[9]

Under U.S. law, a CIA employee or contractor must follow an internal notification process before bringing a complaint to congressional oversight committees. The governing act also provides that such an insider "who intends to report to Congress a complaint or information with respect to an urgent concern may report such complaint or information to the Inspector General."[10] "Urgent concern" in this context means:

- A serious or flagrant problem, abuse, violation of law or executive order, or deficiency relating to the funding, administration, or operations of an intelligence activity involving classified information, but does not include differences of opinions concerning public policy matters
- A false statement to Congress, or a willful withholding from Congress, on an issue of material fact relating to the funding, administration, or operation of an intelligence activity[11]

Insider complaints of this sort are a form of "whistleblowing"—they expose wrongdoing outside of the regular chain of command within intelligence services, but without necessarily sharing secrets outside the narrow confines of government agencies or other approved oversight bodies. The availability of such complaint mechanisms may reduce the likelihood that an employee will resort to more extreme forms of disclosure; for example, to the media.

Quite reasonably, some jurisdictions encourage recourse to this form of whistleblowing. Some, for instance, offer protections to the insider who raises the complaint through these authorized channels. In New Zealand, for instance, "[w]here any employee of an intelligence and security agency brings any matter to the attention of the Inspector General [for Intelligence and Security], that employee shall not be subjected by the intelligence and security agency to any penalty or discriminatory treatment of any kind in relation to his or her employment by reason only of having brought that matter to the attention of the Inspector-General" unless done in bad faith.[12] In the United States, "no action constituting a reprisal, or threat of reprisal, for making such complaint may be taken by any employee of the [Central Intelligence] Agency in a position to take such actions, unless the complaint was made or the information was disclosed with the knowledge that it was false or with willful disregard for its truth or falsity."[13]

In some jurisdictions, internal whistleblowing is a prerequisite to more public, external forms of whistleblowing. In Canada, for instance, a failure to first make a disclosure through internal channels may make it difficult for the complainant to successfully defend himself or herself against criminal charges of unauthorized disclosure of classified information.[14]

2.2 PUBLIC COMPLAINTS

Public complaints are proceedings initiated by persons unconnected to government. These sorts of complaints stand on a different footing to insider complaints. For one thing, the public complainant may be only dimly aware of the wrongdoing at issue. A member of the public wrongly surveilled, for instance, may only find out about this problem by happenstance, and even then may be oblivious to the precise identity of the agency engaged in the surveillance. For these reasons, this person will likely have little concrete information on which to predicate a complaint. It may also be the case that this person comes from a social, ethnic, or religious group disinclined or otherwise deterred from making complaints. A classic example of such a person might be a recent immigrant unfamiliar with the institutions and practices of his or her new host society.

Any public complaints system must, therefore, be accommodating of uncertainty and broadly accessible. This means that there should be broad grounds for public complaints and low barriers to the initiation of investigations in response to complaints.

Some jurisdictions adopt this practice by ensuring that there are no restrictions on the class of persons entitled to make complaints, and by permitting complainants to raise concerns about a broad range of subjects. In the Netherlands, for instance, after notifying the relevant minister to enable the latter to provide his or her views, "each person" may bring complaints to the national ombuds institution in relation to the security services' implementation of their governing law.[15] In Ireland, the Garda Síochána Ombudsman Commission may "receive complaints made by members of the public concerning the conduct of members of the Garda Síochána" (that is, the police).[16] Likewise, in Canada, the most generic complaint that a public complainant may bring against the security intelligence service concerns "any act or thing done by the Service."[17] Finally, in the United States, the Inspector General of the CIA "is authorized to receive and investigate complaints or information from any person concerning the existence of an activity constituting a violation of laws, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety."[18]

These broad formulations of public standing to bring complaints seem desirable if the purpose of the complaint-handling model is to superimpose another means of regulating the legality and probity of intelligence service conduct. Still, a number of other jurisdictions depart from broad public standing concepts and constrain the ability to bring complaints to a class of individual narrower than "any person." Some of these limitations appear modest, but may be quite uncertain in scope. For instance, the Kenyan Complaints Commission may receive complaints from "any person aggrieved" by the intelligence service in the exercise of its powers or performance of its functions.[19] In South Africa, "any member of the public" may make a complaint to the Joint Standing Committee on Intelligence "regarding anything which such member believes that a Service has caused to his or her person or property."[20]

Both of these approaches seem to forestall preemptive or speculative complaints prompted by awareness of a particular intelligence service practice. For example, an ethnic association suspecting ethnic profiling in intelligence investigations may lack standing to bring a complaint, absent a representative complainant with personal experience with such practices. It is difficult to see what value added is produced by this restriction, if the purpose of the complaints system is to regulate legality and probity by the intelligence service.

It is even more problematic when jurisdictions impose nationality rules for some types of complaints. For instance, the New Zealand Inspector-General of Intelligence and Security may only receive complaints from "a New Zealand person" (a citizen or permanent resident) or a person who has been or is employed by one of the intelligence agencies.[21] The Australian Inspector General of Intelligence and Security (IGIS) may only receive complaints concerning the Australian foreign intelligence service from "a person who is an Australian citizen or a permanent resident."[22] (These nationality strictures are not, however, applied in relation to complaints concerning the Australian domestic security intelligence service.)

Nationality (or nationality/residency) rules are an arbitrary barrier to complaints. The result may be to stave a flow of information about the performance of the intelligence service from particularly likely target groups, including refugee claimants and other foreign populations who are not yet permanent residents or citizens. Again, to the extent that complaints serve as early warning indicators of wrongdoing, it is difficult to see what virtue flows from limiting standing in this manner.

3. VENUES FOR COMPLAINTS

This section deals with the place to which complaints may be brought. The institutions to which complaints are brought vary. Speaking generally, these institutions can be subdivided into two broad classes: general venues and specialized venues. By "general venues," this tool means institutions *without* a specialized security or intelligence oversight mandate. Examples of general venues include the courts, ombuds institutions, national human rights commissions, and other regulatory bodies such as data commissioners. "Specialized venues," on the other hand, are institutions specifically mandated to deal with security or intelligence issues. Examples include expert oversight bodies such as Belgium's Committee I and Canada's SIRC.

3.1 GENERAL VENUES

3.1.1. Regular courts

In some jurisdictions, the regular civil courts are competent to hear a complaint related to the intelligence services, grounded as recognizable forms of civil wrongs (including various forms of torts). In others, administrative courts may hear cases within their own subject-matter jurisdiction (i.e., administrative law) that concern the actions of the intelligence services.[23]

In fact, in at least some (and perhaps most) jurisdictions, courts of some sort constitute the only venue competent to receive complaints concerning the intelligence services.[24] There are no specialized intelligence oversight bodies authorized to receive complaints. Such a choice presents challenges. As discussed below, courts may be competent to award potent remedies, but for practical reasons it may also be near impossible for a complainant to obtain such a remedy: the sometimes unique complaints about intelligence services are squeezed within the conventional jurisdiction of regular courts (e.g., as an actionable civil wrong) or are not heard at all.

3.1.2. Conventional regulatory bodies

It is also notable that like other government institutions, intelligence services fall under the jurisdiction of institutions with either general mandates to handle complaints about public bodies or subject-matter mandates that are not specific to intelligence services. These institutions include ombuds institutions, data protection commissions, and human rights commissions. They may, for instance, be competent to hear complaints concerning the use of information by intelligence services, or their human rights compliance more generally. In the Netherlands, for example, complaints may be brought to the national ombudsman about the actions of, among other things, the relevant ministers, heads of the General Intelligence and Security Service or the Defence Intelligence and Security Service and the persons working for these entities.[25] Likewise, in Finland and Sweden, complaints concerning the security police may be brought to the parliamentary ombuds institution.[26] In Belgium, Finland, and Canada, the privacy (or data) commissioner may receive complaints concerning treatment of personal information by the intelligence services.[27]

In some jurisdictions, subject-matter specific regulatory bodies are required by law to consult with the specialized intelligence oversight and complaint-handling bodies discussed in the next section, if the complaint concerns intelligence services and/or national security matters. In Canada, for instance, the Canadian Human Rights Commission must refer complaints concerning practices "based on considerations relating to the security of Canada" to SIRC. The latter then investigates and reports to the Commission, which decides whether to proceed with the complaint.[28] Bifurcation of this sort necessarily complicates cases, but does serve to centralize the handling of classified information in fewer hands. At the same time, complaint handling is less likely to be undermined by the unwillingness of intelligence services to share classified information with the conventional regulatory bodies.

3.1.3. Disadvantages of general venues

A common concern with general types of venues—be they courts or conventional regulatory bodies—is access to classified information. In some jurisdictions, civil courts may be empowered to award successful plaintiffs with damages where intelligence services have committed civil wrongs, but in practice civil suits in the regular courts are made difficult by government claims of secrecy. Since the plaintiff bears the onus of proving the civil wrong, control over the relevant facts by the government may make a successful civil lawsuit near impossible.[29] Likewise, conventional regulatory bodies not specifically tasked with intelligence and national security matters may suffer from an inability to access and review classified information when investigating complaints relating to intelligence services. For instance, the general public complaint-handling body for Canada's national police force, the Royal Canadian Mounted Police, has repeatedly complained of its inability to probe the police's national security-related activities because of secrecy.[30]

It may also be the case that general venues are *too* general; that is, they lack expertise in dealing with security and intelligence services. As a consequence, they may be more deferential to intelligence services' claims of secrecy or other forms of special circumstance than are more expert oversight bodies with long experience in overseeing such services.

Last, the very nature of the complaints brought about intelligence services may render conventional courts or regulatory bodies ill-equipped to handle them. Complainants will

often be obliged to fit particular complaints about legality or probity of conduct into standard civil or regulatory grounds for complaint. The fit may be poor, and otherwise meritorious complaints may be dismissed, not because they do not raise real doubts about the intelligence service, but because those doubts cannot be articulated in the jurisdictional language of the general complaint-handling body. Illicit surveillance, for example, may not be recognized as a civil wrong in some jurisdictions, and thus may not lie within the purview of conventional courts.

3.2 SPECIALIZED VENUES

An obvious response to the shortcomings of general venues is to create more specialized complaint-handling fora. Specialized venues normally fit into one of three categories: first, they may be internal to the executive branch (e.g., some inspectors general); second, they may be independent from the executive branch and parliament; finally, they may be parliamentary bodies.

3.2.1 Internal complaint-handling bodies

Some jurisdictions have internal watchdogs, which serve as a means for the political executive to oversee intelligence services. These bodies may simply be an individual minister or a special ministerial delegate, sometimes called an inspector general. It should be noted, however, that, in some jurisdictions, the inspector general is a truly independent entity—that is, he or she has a security of tenure and independence of operation that places the inspector beyond the command and control of the executive and the intelligence services. In some instances, internal bodies may be competent to receive public complaints.[31] From the executive's perspective, such an approach minimizes the need to share classified information that may be at issue in a complaint, outside of very narrow confines. At the same time, internal complaint-handling bodies lack independence and autonomy from those responsible for the intelligence services. The public may perceive such bodies to be susceptible to conflicts of interest stemming from the "fox guarding the henhouse," and may prompt doubts about the legitimacy of an internal complaint-handling process.

3.2.2 Independent complaint-handling bodies

Structure

More independent but still narrowly specialized complaint-handling bodies represent an obvious compromise between the need to limit the dissemination of classified information and at the same time foster public legitimacy. A number of jurisdictions have established expert oversight bodies staffed and operated independently from the intelligence services and the rest of executive branch. These agencies enjoy the credibility that stems from independent operation. Yet they may, nevertheless, be sufficiently proximate to government that their members may be security cleared and trusted with classified information. This was exactly the practice codified in the law governing one of the first such bodies, Canada's SIRC, in an effort to allay intelligence service concerns about the flow of classified information. The SIRC's members are appointed by the federal executive, but after consultation with the opposition parties in parliament. Members enjoy substantial security of tenure for renewable terms of five years and engage their own staff, albeit with the approval of the financial management branch of the executive

government. Each member swears an oath of secrecy and is subject to Canada's official secrets law.[32]

While the Canadian system does not oblige appointment of individuals with particular expertise, other jurisdictions apply a different approach. For instance, the Kenyan intelligence service's Complaints Commission is chaired by a judge and comprises four other members, one of whom is an "advocate" of not less than seven years' standing and one of whom must be a "religious leader" of "national repute." The commissioners are appointed by the president, "on the advice of the Judicial Service Commission" and "shall hold office for a period of three years," subject to reappointment for up to two terms.[33] For its part, the Belgian Committee I is appointed by the senate for renewable six year terms and its members must meet certain qualifying criteria in terms of legal knowledge and relevant experience, and they may not be members of a police or intelligence service.[34]

It is difficult to assess the bona fides of such independent appointment systems from a distance. However, the principle is a sound one. Moreover, appointment systems that impose competence and professional background expectations are warranted, if these do not have the effect of creating an exclusive caste of appointees. Overly narrow and demanding appointment criteria may confine the class of suitable persons to those with intelligence backgrounds—a development that would lead to the perception (if not the reality) of "capture" of the oversight body by the intelligence service subject to the oversight.

The UK Investigatory Powers Tribunal represents an example of a quite different set of professional expectations: it is staffed exclusively by persons who have held high judicial office or have been lawyers for at least ten years.[35] Yet, a membership comprising only lawyers and former judges may also be extreme. There is some merit to staffing a body serving a broad public interest in a manner that reflects a range of perspectives and professional pedigrees.

This is the philosophy that appears to animate Canada's SIRC: there are no professional prerequisites for membership. Rather, its members must simply be members of the Privy Council of Canada who are not currently in the federal legislature. In practice, the pool of potential appointees includes former senior politicians, leading judges, and "distinguished" individuals singled out for this honour. It is entirely possible that a person will be appointed to the Privy Council for the very purpose of then becoming a member of SIRC. Put another way, membership in SIRC is wide open, enabling that body (at least in principle) to represent the broader public which it serves.

The flexibility of the Canadian approach may, however, err too far. It seems disingenuous to staff a complaint-handling body charged with a quasi-judicial function entirely with non-lawyers, an eventuality that is currently true of Canada's SIRC. Whatever the other qualities of members, the lack of legal training may create a dependence on the complaint-handling body's legal staff. This is a development that, in turn, requires careful assessment of the career trajectory of these legal staff and their movements between and among government bodies (including, potentially, the intelligence services). The independence of a complaint-handling body may be impaired (or perceived as being impaired) where members are dependent on career public servants who move in and out of executive government. In view of this, the ideal model may be a multi-member complaint-handling

body staffed by persons of diverse backgrounds, but ensuring that a minimum quota of such members have, e.g., legal training.

Function

Some jurisdictions have established oversight bodies whose sole function is to receive and investigate complaints. For instance, in the United Kingdom, the Investigatory Powers Tribunal "can investigate complaints about any alleged conduct by or on behalf of the Intelligence Services - Security Service (sometimes called MI5), the Secret Intelligence Service (sometimes called MI6) and GCHQ (Government Communications Headquarters)."[36]

In other instances, the chief function of these expert oversight bodies is to review intelligence services' performance, either independently or at the behest of ministers or parliamentarians.[37] However, these bodies may also be authorized to receive (and investigate) complaints concerning the intelligence services they are mandated to oversee.[38] In Norway, for instance, the Parliamentary Intelligence Oversight Committee is a body whose members, while elected by the parliament, are not institutionally part of the legislative branch. As well as investigating the activities of the intelligence services on its own initiative, the Committee may also receive and investigate complaints from members of the public.[39] Likewise, Belgium's Committee I "deals with the complaints and denunciations it receives with regard to the operation, the intervention, the action or the failure to act of the intelligence services, the Coordination Unit for Threat Assessment, and the other supporting services and their personnel."[40] Similar functions are performed by the South African Inspector-General of Intelligence (IGI)—an office that is independent from the executive and accountable to the parliamentary oversight committee noted below. The inspector general may "receive and investigate complaints from members of the public and members of the Services on alleged maladministration, abuse of power; transgressions of the Constitution, laws and policies [on intelligence and counter-intelligence], corruption and improper enrichment of any person through an act or omission of any member."[41]

In some jurisdictions, complaints to these expert oversight bodies must be preceded by notification of the intelligence service. In Canada, for instance, a public complaint must be directed first to the CSIS director. The SIRC may then investigate non-frivolous, good faith complaints if the director fails to respond in a period of time the committee views as reasonable, or provides an inadequate response.[42]

3.2.3 Parliamentary complaint-handling bodies

A number of jurisdictions have special parliamentary bodies that oversee intelligence and services. As with some of the expert oversight bodies described above, these parliamentary committees may also be charged with receiving and investigating complaints concerning intelligence service activities.[43] In Germany, for instance, the parliamentary control panel may hear complaints.[44] In South Africa, the parliamentary Joint Standing Committee on Intelligence (a body comprising fifteen members of parliament that performs an intelligence service oversight function) does not investigate complaints directly but it may:

> *[O]rder investigation by and to receive a report from the Head of a Service or the Inspector-General regarding any complaint received by the Committee from any member of the public regarding anything which such member believes that a Service has caused to his or her person or property: Provided that the Committee is satisfied that such complaint is not trivial or vexatious or made in bad faith.*[45]

Charging parliamentary committees with both oversight and complaint-handling functions enables the concentration of security sector-related expertise in a single body, while at the same time limiting the dissemination of classified information. There are however, a number of drawbacks associated with giving parliamentary oversight bodies a complaint-handling function. First, parliamentarians may not have sufficient expertise or time to investigate and adjudicate complaints. Second, parliamentarians are, by definition, partisan actors. This may compromise their capacity to investigate and adjudicate properly complaints that raise particularly acute sensitivities about the conduct of incumbent governments. Third, complaint handling may require close scrutiny of minutiae, rules of procedural fairness, and evidentiary considerations relating to, e.g., the credibility of witnesses, which are better handled in a more quasi-judicial environment. Finally, parliamentary committees often have large memberships, which may make reaching and articulating clear adjudicative judgments difficult.

4. COMPLAINT-HANDLING PROCEDURES AND THE CONTROL OF INFORMATION

It is not possible in this short tool to describe in detail complaint-handling procedures. The focus will, therefore, be on a few general procedural considerations, as well as the procedures used for protecting classified information. Since procedures deployed by bodies with more general mandates (i.e., mandates that go beyond intelligence services) are highly variable, the focus in this section is on the procedures applied by the specialized (intelligence and national security-related) complaint-handling bodies (CHBs) discussed in Section 3.2 above.

4.1 GENERAL PROCEDURAL RULES

The governing legislation of some jurisdictions provides that complaints must be in writing.[46] CHBs may be empowered to dismiss complaints judged frivolous, vexatious, made in bad faith, or otherwise falling below a *de minimis* threshold for triggering an investigation.[47] Such a limitation obviously limits the effect of broad standing rules, allowing the body to dismiss plainly non-meritorious complaints. Of course, if applied too sweepingly to sidestep difficult cases, such rules could render a complaint-handling body ineffective in performing oversight and complaint-handling functions. Ultimately, the safeguard for proper use of these filtering rules lies in the independence of the body itself. Staffed properly by attentive, skilled persons sufficiently autonomous of government, there will be little incentive to dispense with controversial cases on putative procedural grounds.

It is very important that CHBs do not confuse complaints that are "frivolous and vexatious" with those that are not "not accompanied by sufficient details." As already noted, complaints challenging the conduct of a surreptitious and secretive intelligence service might reasonably be expected to lack the ample details associated with more open proceedings. Likewise, "bad faith" grounds of dismissal should not be deployed simply in response to difficult complainants. Mounting a complaint against a powerful intelligence service is a daunting prospect that is likely to deter all but the most stubborn. Complainants—and especially whistleblowers—may have idiosyncratic qualities that lead observers to question the legitimacy of their complaint. Special care needs to be exercised in parsing fact from personality qualities that may raise doubts about credibility.

Where hearings or inquiries are held, the rules governing at least some CHBs impose standards of procedural fairness, requiring for instance that affected parties be heard before findings impugning the conduct of these persons are made.[48]

4.2 POWERS OF COMPLAINT-HANDLING BODIES

Some CHBs have the powers to compel the production of documents and the presence of witnesses.[49] Such powers may, in some instances, be quite sweeping and may supersede such things as lawyer-client privileges.[50] For example, SIRC may have access to all information in possession of the intelligence service, excluding cabinet confidences (essentially records of cabinet deliberations). Elsewhere, in the United States, the Inspector General of the CIA

> *[S]hall have access to any employee or any employee of a contractor of the Agency whose testimony is needed for the performance of his duties. In addition, he shall have direct access to all records… which relate to the programmes and operations with respect to which the Inspector General has responsibilities ... Failure on the part of any employee or contractor to cooperate with the Inspector General shall be grounds for appropriate administrative actions by the Director, to include loss of employment or the termination of an existing contractual relationship.*[51]

For other CHBs, access to information is more circumscribed. In South Africa, the governing legislation bars the parliamentary Joint Standing Committee on Intelligence from access to information that might reveal the identity of the intelligence service's informants.[52] (On the other hand, the South African IGI operates under fewer restrictions—no access to intelligence, information or [security service] premises may be withheld from the inspector-general "on any ground.")[53] Limiting complaint-body access to secret information is an obvious effort to limit the prospects of voluntary or involuntary leaks. Yet, limitations may impair the ability of the complaint-handling body to assess the merits of the complaint thoroughly. Put another way, it may handicap the CHB from inception. This is therefore a concern if the intent is to create a meaningful CHB.

A partial solution to the conundrum of information security is to prescribe information-handling expectations in the rules governing CHBs.[54] The South African IGI, for instance, must "comply with all security requirements applicable to the employees of the intelligence services."[55] In Canada, SIRC members are bound by Canada's official secrets law, and thus subject to prosecution should they wrongfully reveal secret information.[56]

Protocols are also in place to control the physical flow of information. For example, SIRC researchers generally review classified information in secure SIRC offices at CSIS's own facilities. There will be some instances, however, where information is moved to SIRC's own secure facilities, not least in instances where that information is at issue in complaints adjudicated before SIRC. Creating this information-handling infrastructure may require a substantial investment and in a geographically large country (like Canada) may limit the places in which SIRC will conduct its proceedings.

4.3 NATIONAL SECURITY CONFIDENTIALITY

As the discussion above suggests, the professional handling of national security-related information is a cardinal preoccupation in any complaint-handling system. The legislation governing many CHBs specifies that inquiries and/or hearings must be conducted in

private.[57] In addition, the findings of CHBs may be redacted and/or their dissemination may be restricted. For instance, in Australia, the IGIS must not provide findings to the complainant "until the head of the relevant [intelligence] agency and the Inspector General have agreed that the giving to the complainant of a response in the terms proposed will not prejudice security, the defence of Australia or Australia's relations with other countries."[58] In South Africa also, the IGI may not release restricted information without advance permission from the government.[59] Likewise, in Kenya, the Complaints Commission must "have regard to the requirements of national security" in the discharge of its functions. To this end, it must consult with the director-general of the National Security Intelligence Service (and the ministerial-level National Security Council) "in determining information or circumstances under which certain information may not be disclosed in the course of or in relation to any inquiry in the interests of national security."[60] In Norway, the Committee's statements to complainants "should be as complete as possible without revealing classified information."[61]

Because secrecy may impair the capacity of the complainant to bring a complaint successfully, some jurisdictions may employ special procedures in closed portions of hearings to assist the complainant. In Canada, for instance, SIRC counsel are charged with

> *[C]hallenging decisions on the non-disclosure of the information contained in the closed material, as well as cross-examining government witnesses in closed proceedings. … Outside counsel (or 'legal agents') may be retained in some cases where, because of workload issues, inside counsel is not fully capable of acting in the adversarial proceedings. In other cases, legal agents may be retained where inside counsel judge that the case will require particularly aggressive cross-examination of CSIS.*[62]

5. REMEDIES

As noted above, the central purpose of any complaints system is an "effective remedy." Notably, the remedies offered by intelligence service complaint-handling bodies often amount to recommendations rather than binding legal determinations relating to, e.g., the award of damages.[63] These limited powers likely reflect the dual mandate of many CHBs; that is, the body hearing complaints is one and the same as the body that conducts autonomous oversight of intelligence services' activities. These oversight processes normally generate recommendations to the intelligence service concerned and the executive branch on reforming policies and practices. Where oversight constitutes the primary function of the CHB, the legislators who created these institutions likely regarded the availability of coercive compensation powers in response to complaints as inconsistent with the less adversarial qualities required for effective oversight.

In practice, however, restricting CHBs to making recommendations may limit their capacity to do more than shame an intelligence service into compliance. This approach may be especially difficult where the results of investigations of complaints are themselves classified, a commonplace practice noted above. For this reason, there is merit in CHBs producing redacted versions of their findings, in publicly available annual reports or otherwise. Even these, however, may draw surprisingly little attention from parliamentarians and the media. Canada's SIRC, for example, has issued summaries of sometimes damning findings that spark little sustained interest.

In the worst instances, a power merely to recommend may have the effect of reducing whatever other virtues a CHB has. If potential complainants doubt that their actions will result in meaningful responses, change, or compensation, they may have little reason to pursue a complaint with the CHB. Consequently, complainants may seek to bring their grievances through other channels (like generalist courts ill-positioned to deal with them), disclose them to the media in the hope of animating a response, or simply abandon their efforts. All of these responses undermine the rationale for the CHB: to reveal and respond to wrongdoing by the intelligence services.

Other bodies have more "judicial-like" powers. This is especially true of CHBs for which complaint-handling is their exclusive occupation. Thus, quasi-judicial bodies, such as the UK Investigatory Powers Tribunal, have the power to impose "[r]emedial measures such as the quashing of any warrants, destruction of any records held or financial compensation."[64]

6. RECOMMENDATIONS

A number of recommendations flow from this survey of complaint-handling bodies. These are summarized in the discussion that follows and proposed as "best practices" in Table 1.

- States should create complaint-handling bodies tasked with receiving and investigating both insider and public complaints.

Insider complaint-handling systems constitute a means of directing "whistleblowing" through an institutional framework that is both responsive to meritorious complaints and can accommodate government concerns regarding the protection of classified information. However, this system should also extend protections to those who follow it.

- An effective insider complaints system should include guarantees of non-retaliation where employees bring good faith claims to authorized bodies.

Public complaints systems, in comparison, are broader and generally open to all persons. A few jurisdictions do impose nationality requirements, although generally only in relation to foreign intelligence operations, and even fewer require that the complainant be personally affected in some way by the subject matter of the complaint. It is difficult to see any real merit to limiting standing in these ways.

- Complaint-handling bodies should have broad competence to receive complaints from the public.

Broad rules regarding who has standing to bring a complaint mean more complaints can be directed to the complaint-handling body. Such rules also expand the potential burden on that entity. It may be appropriate to limit these cases to only those that have merit. But care should be taken in how this determination is made.

- Concerns about frivolous or vexatious complaints may be remedied by rules allowing the complaint-handling body to dismiss such complaints early in the process. But caution should be exercised to avoid dismissing complaints that are difficult, politically controversial, or simply brought by difficult people.

In terms of venue, states should consider carefully whether general courts or conventional regulatory bodies are adequately equipped to deal with complaints relating to intelligence services. In practice, these bodies may be unable to deal with classified national security and/or intelligence material, with the result that their effectiveness is impaired and they are unable to adequately investigate complaints. Further, generalist bodies may lack the subject-matter expertise required to investigate these matters with a high degree of thoroughness.

In comparison, intelligence-specific complaint-handling bodies may be structured to accommodate concerns about the protection of classified information. At the same time, these secrecy concerns should not have the effect of abasing the functions of the specialized complaint-handling body to the point where its credibility as a complaint-handling body evaporates. Transparency should be the default, with secrecy limited to bona fide circumstances. More than this, there should be efforts to ensure some parity between the government's and complainant's abilities to present their cases. Where the government may mask its positions through secrecy, the body itself should be sure to probe the matter in an inquisitorial manner. Further, the oversight body's members themselves should be security cleared and should have sweeping access to information in the possession of the government and the intelligence services.

- In most instances, specialized complaint-handling bodies are to be preferred over more general complaint handling for investigating complaints relating to intelligence services. Such bodies should be equipped with very broad powers to access classified information, and they should be required to implement safeguards to reduce the prospect that this information will be leaked (voluntarily or involuntarily). Examples of such safeguards include special information-handling protocols and affirmative security-clearance obligations.

That said, complaint-handling bodies will only be credible where staffed and maintained independently of government and adequately resourced. While complaint-handling bodies should not comprise exclusively those with particular professional pedigrees (e.g., lawyers), there should be adequate legal representation among the membership. Independent legal competency minimizes what might otherwise be excessive dependence on legally trained (and perhaps not quite as independent) staff members.

- Complaint-handling bodies must be independent of government. In practice, this means that they are appointed in a manner that does not constitute unilateral appointment by incumbent governments and that they are free to operate autonomously of government, while enjoying security of tenure. At least some members should be legally trained to avoid excessive dependence on intelligence service staff in the adjudication of complaints.

The question of remedies is the most difficult issue in complaint-handling systems. Speaking generally, the bodies with the most potent ability to compensate for intelligence service wrongdoing (courts) are the least well equipped to deal with complaints relating to the special circumstances surrounding intelligence services, particularly the demands of secrecy and protection of classified information. Expert oversight bodies are often better equipped to penetrate the fog of secrecy but generally have no power to do more than make recommendations. States should consider carefully whether expert oversight

bodies vested with complaint-handling functions should also have quasi-judicial remedy powers, such as the power to award financial compensation to wronged individuals.

- Equipping complaint-handling bodies with mere powers of recommendation is insufficient and does not constitute an "effective remedy." Instead, these bodies should be given quasi-judicial remedy powers, such as the power to award financial compensation.

Lastly, states should avoid exclusive dependence on a complaint-based model to ensure intelligence service accountability. Complaint handling has its place in this process; however, the experience of some states that rely exclusively on complaint-handling bodies to perform this function has not been positive. In Canada, for example, the national security functions exercised by the federal police (the RCMP) are subject to only to a weak, complaint-based accountability mechanism. A judicial inquiry into RCMP's doubtful anti-terrorism practices in the aftermath of 9/11 recommended both a bolstered complaint-handling power and a performance auditing review system. The inquiry reasoned that "[t]he need for self-initiated reviews stems from the fact that most of the RCMP's national security activities are conducted in secret and receive little, if any, judicial scrutiny, yet have the potential to significantly affect individual rights and freedoms."[65]

A myopic focus on complaint-based accountability models risks creating a form of accountability "theatre": the existence of the body creates the appearance of checks and balances but it cannot operate effectively because of the secrecy surrounding intelligence service activity. This secrecy may leave those targeted by intelligence services oblivious to, e.g., unauthorized encroachments on privacy. For this reason, systems of complaint handling unaccompanied by other forms of review and oversight, capable of exposing wrongdoing, represent a poor approach to intelligence governance.

- Exclusive dependence on a complaint-based model of intelligence service accountability is inadequate. Such an approach must be supplemented by a system of independent review and/or oversight.

TABLE 1: BEST PRACTICES CHECKLIST ON COMPLAINT HANDLING	
Practice	Implications of failing to follow the practice
Is the CHB adequately equipped with subject matter and legal expertise?	If not, questions may be raised about the CHB's ability to adjudicate complaints effectively and credibly.
Does the CHB enjoy full access to intelligence service secret information?	If not, the CHB risks being unable actually to determine the merits of complaints and assess the conduct of the service.
Does the CHB enjoy independence from the government and intelligence service in terms of the process of appointment, security of tenure, and management of operations?	If not, the CHB will likely lack credibility and may, in fact, not render independent decisions.
Does the CHB allow both insider and public complaints?	If not, insiders may be prompted to resort to whistleblowing in, e.g., the media, while members of the public are left to bring complaints in generalist courts or other bodies ill-equipped to adjudicate national security matters.
Are insider complainants protected from retaliation when making good-faith complaints, either under employment law and/or official secrets law?	If not, insiders will have no incentive to follow the CHB process, or will be deterred from revealing wrongdoing at all.
Is the jurisdiction over public complaints broadly phrased to allow all and any member of the public to bring a complaint on the full breadth of intelligence service activities?	If not, legitimate concerns about intelligence service behaviour may go unremarked.
While a competence to dismiss non-meritorious claims is appropriate, is the CHB careful to exercise that power prudently and without an eye to extraneous considerations like the political implications of the complaint or irrelevant qualities of the complainant?	If not, legitimate concerns about intelligence service behaviour may be dismissed too readily.
Does the CHB have the power to issue quasi-judicial remedies, such as financial compensation?	If not, the CHB's determinations may have little impact on intelligence service behaviour, while complainants may be deterred from bringing complaints in the first place.

Endnotes

1. Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Geneva: DCAF, University of Durham, and Parliament of Norway), p. 105.
2. Hans Born and Ian Leigh, *Democratic Accountability of Intelligence Services*, Policy Paper No. 19 (Geneva: DCAF, 2006) p. 17.
3. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: 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* (henceforth Scheinin Report), United Nations Document A/HRC/14/46 (17 May 2010), p. 10.
4. Scheinin Report, p. 10.
5. Scheinin Report, p.11 (citing Article 2 of the International Covenant on Civil and Political Rights).
6. Klass v. FRG, A 28 (1979), 2 EHHR 214 at para. 64 (construing Art 13 of the ECHR).
7. Scheinin Report, p. 11.
8. Canadian Security Intelligence Service Act (31 August 2004), R.S.C., Chapter C-23, Section 42 (available at http://www.csis-scrs.gc.ca/pblctns/ct/cssct-eng.asp).
9. Belgium, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18 July 1991), Articles 28 and 30 (available at http://www.comiteri.be/images/pdf/engels/w.toezicht - l.contrle - engelse versie.pdf).
10. United States, Inspector General for the Central Intelligence Agency, U.S. Code 50, §403q (e)(2) (available at http://codes.lp.findlaw.com/uscode/50/15/I/403q).
11. United States, Inspector General for the Central Intelligence Agency, U.S. Code 50, §403q (d)(5)(G).
12. New Zealand, Inspector-General of Intelligence and Security Act (1 July 1996), Section 18 (available at http://www.legislation.govt.nz/act/public/1996/0047/latest/whole.html - dlm392526).
13. United States, Inspector General for the Central Intelligence Agency, U.S. Code 50, §403q (e)(3)(B).
14. Canada, Security of Information Act (1985), R.S.C., Chapter O-5, Section 15 (available at http://laws.justice.gc.ca/eng/acts/O-5/).
15. The Netherlands, Intelligence and Security Services Act (7 February 2002), Article 83 (as amended) (available at http://www.ctivd.nl/?download=WIV 2002 Engels.pdf).
16. Ireland, Garda Síochána Act 2005, No. 20 of 2005, Section 67.
17. Canadian Security Intelligence Service Act (31 August 2004), R.S.C., Chapter C-23, Section 41 (available at http://www.csis-scrs.gc.ca/pblctns/ct/cssct-eng.asp).
18. United States, Inspector General for the Central Intelligence Agency, U.S. Code 50, §403q (e)(3).
19. Kenya, National Security Intelligence Service Act (31 December 1998), Section 24 (available at http://www.nsis.go.ke/act.pdf).
20. South Africa, Intelligence Services Oversight Act (23 November 1994), Section 3 (1) (f) (available at http://www.acts.co.za/intelligence_services_oversight_act_1994.htm).
21. New Zealand, Inspector-General of Intelligence and Security Act (1 July 1996), Section 11.
22. Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 8 (available at http://www.comlaw.gov.au/Details/C2011C00349).
23. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, United Nations Document A/HRC/14/46/Add.1 (26 May 2010), p. 50 (discussing Finland).
24. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, United Nations Document A/HRC/14/46/Add.1 (26 May 2010) Paragraph 121 (naming the complaints mechanism for Benin as the constitutional court); Paragraph 294 (naming the chief complaints venue for Ecuador as the constitutional court); Paragraph 243 (same, in relation to Costa Rica); Paragraph 307 (naming courts as the chief complaints mechanism for a person aggrieved by surveillance by the security service); Paragraph 353 (discussing the role of courts in relation to civil wrongs committed by the intelligence services of Georgia, and of the chief prosecutor in relation to criminal wrongdoing), Paragraph 482 (discussing the system in Latvia); Paragraphs 556–557 (discussing the system in Madagascar).
25. The Netherlands, Intelligence and Security Services Act, Article 83.
26. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and*

protection of human rights and fundamental freedoms while countering terrorism: Addendum, United Nations Document A/HRC/14/46/Add.1 (26 May 2010), p. 49 (discussing Finland); Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *International Models of Review of National Security Activities* (May 2005), p. 14 (available at http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/IntlModels_may26.pdf).

27. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, United Nations Document A/HRC/14/46/Add.1 (26 May 2010), Paragraphs 67, 75, and 82 (discussing Belgium); Paragraph 327 (discussing Finland); Paragraph 374 (describing the roles of the Greek ombuds institution); see also, Canada, Privacy Act (1985), R.S.C., Chapter P-21, Section 29 (available at http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html).
28. Canadian Human Rights Act (1985), R.S.C., Chapter H-6, Sections 45–46 (available at http://laws-lois.justice.gc.ca/eng/acts/H-6/page-15.html).
29. For court cases in which governmental secrecy claims have impaired (or at least complicated) plaintiffs' capacity to obtain civil remedies, see *Mohamed v. Secretary of State for Foreign and Commonwealth Affairs*, [2009] EWHC 152 (Admin) (UK); Mohamed v. Secretary of State for Foreign and Commonwealth Affairs [2009] EWHC 2549 (Admin) (UK); *Canada (Attorney General) v. Almalki*, 2011, FCA 199 (Canada); *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070 (9th Cir. Cal. 2010) (United States).
30. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (2006), pp. 492–3 (available at http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/EnglishReportDec122006.pdf).
31. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, United Nations Document A/HRC/14/46/Add.1 (26 May 2010), Paragraph 380 (describing the competency of the responsible Hungarian minister to receive complaints concerning the activities of the Hungarian security agencies); Paragraphs 521–523 (discussing the internal control system in Macedonia); and United States, Inspector General for the Central Intelligence Agency, U.S. Code 50, §403q.
32. Canadian Security Intelligence Service Act (31 August 2004), R.S.C., Chapter C-23, Sections 35–37.
33. Kenya, National Security Intelligence Service Act (31 December 1998), Section 25.
34. Belgium, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18 July 1991), Articles 28 and 30.
35. United Kingdom, Investigatory Powers Tribunal web site (available at http://www.ipt-uk.com/default.asp?sectionID=1).
36. United Kingdom, Investigatory Powers Tribunal web site, "About IPT: What the Tribunal can investigate" (available at http://www.ipt-uk.com/sections.asp?sectionID=22&type=top).
37. The Netherlands, Intelligence and Security Services Act, Articles 64 and 78.
38. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, United Nations Document A/HRC/14/46/Add.1 (26 May 2010) Paragraphs 270 and 271 (describing the functions of the Croatian Council for Civil Oversight of the Security Intelligence Agencies); Paragraph 279 (describing the functions of the Cypriot Independent Authority for the Investigation of Allegations and Complaints Against the Police); Paragraph 396 (describing the functions of the Irish Garda Síochána Ombudsman Commission); Paragraph 410 (describing the functions of the Japanese Prefectural Public Safety Commission); Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 8 (as amended).
39. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, United Nations Document A/HRC/14/46/Add.1 (26 May 2010) Paragraph 585; Norway, Act Relating to the Monitoring of Intelligence, Surveillance, and Security Services (3 February 1995), Section 3 (available at http://www.eos-utvalget.no/filestore/EOSAct.pdf).
40. Belgium, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18 July 1991), Article 34.
41. South Africa, Intelligence Services Oversight Act (23 November 1994), Section 7(7)(cA).
42. Canadian Security Intelligence Service Act (31

August 2004), R.S.C., Chapter C-23, Section 41.

43. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, United Nations Document A/HRC/14/46/Add.1 (26 May 2010) Paragraph 270 (describing the role of the Croatian parliamentary Committee for Internal Policy and National Security); Paragraph 380 (describing the role of the Hungarian parliament's National Security Committee); and Paragraphs 609–611 (describing the Romanian joint parliamentary commissions, but suggesting it will investigate complaints only with the blessing of other parliamentary committees); Larry Watts, "Control and Oversight of Security Intelligence in Romania," in *Democratic Control of Intelligence Services*, eds. Hans Born and Marina Caparini (Aldershot, UK: Ashgate, 2007), p. 60 (discussing complaints heard by the Romanian parliamentary committees).
44. DCAF, Backgrounder: Parliamentary Oversight of Intelligence Services (2006) (noting that the German parliamentary "Control Panel" may hear citizen complaints); Germany, Control Panel Act (29 July 2009), *Federal Law Gazette I*, p. 2346, Section 8.
45. South Africa, Intelligence Services Oversight Act (23 November 1994), Section 3(1)(f).
46. Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 10 (as amended); New Zealand, Inspector-General of Intelligence and Security Act (1 July 1996), Section 16.
47. Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 11 (as amended); South Africa, Intelligence Services Oversight Act (23 November 1994), Section 3(1)(f); New Zealand, Inspector-General of Intelligence and Security Act (1 July 1996), Section 17; Belgium, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18 July 1991), Article 34.
48. Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 19 (as amended).
49. Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 18 (as amended); Norway, Act Relating to the Monitoring of Intelligence, Surveillance, and Security Services (3 February 1995), Sections 4 and 5; Germany, Control Panel Act (29 July 2009), *Federal Law Gazette I*, p. 2346, Section 5; New Zealand, Inspector-General of Intelligence and Security Act (1 July 1996), Sections 20 and 23; Kenya, National Security Intelligence Service Act (31 December 1998), Section 26; Belgium, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18 July 1991), Article 48.
50. Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 18 (as amended).
51. United States, Inspector General for the Central Intelligence Agency, U.S. Code 50, §403q (e)(2). See, also, paragraphs (4) and (5).
52. South Africa, Intelligence Services Oversight Act (23 November 1994), Section 5.
53. South Africa, Intelligence Services Oversight Act (23 November 1994), Section 7.
54. South Africa, Intelligence Services Oversight Act (23 November 1994), Section 7; Germany, Control Panel Act (29 July 2009), *Federal Law Gazette I*, p. 2346, Section 10.
55. South Africa, Intelligence Services Oversight Act (23 November 1994), Section 7; See similar strictures in Norway, Act Relating to the Monitoring of Intelligence, Surveillance, and Security Services (3 February 1995), Section 9; New Zealand, Inspector-General of Intelligence and Security Act (1 July 1996), Section 13.
56. Canada, Security of Information Act (1985), R.S.C., Chapter O-5, schedule.
57. Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 17 (as amended); New Zealand, Inspector-General of Intelligence and Security Act (1 July 1996), Section 19; Kenya, National Security Intelligence Service Act (31 December 1998), Section 26.
58. Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 23 (as amended).
59. South Africa, Intelligence Services Oversight Act (23 November 1994), Section 5.
60. Kenya, National Security Intelligence Service Act (31 December 1998), Section 26.
61. Norway, Instructions for Monitoring of Intelligence, Surveillance and Security Services (EOS), Issued pursuant to section 1 of Act No. 7 of 3 February 1995 relating to the Monitoring of Intelligence, Surveillance and Security Services, Section 8; See also New Zealand, Inspector-General of Intelligence and Security Act (1 July 1996), Section 25.
62. Craig Forcese and Lorne Waldman, "Seeking Justice in an Unfair Process: Lessons from Canada, the United Kingdom, and New Zealand on the Use of 'Special Advocates' in National Security Proceedings" (study commissioned by

the Canadian Centre for Intelligence and Security Studies, with the financial support of the Courts Administration Service) (August 2007), pp. 7–8.

63. Canadian Security Intelligence Service Act (31 August 2004), R.S.C., Chapter C-23, Section 52 (describing powers of SIRC); Netherlands, Intelligence and Security Services Act, Article 84 (describing powers of National Ombudsman); United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, United Nations Document A/HRC/14/46/Add.1 (26 May 2010) Paragraph 77(describing the powers of the Belgian privacy commissioner); and Paragraph 585 (describing the powers of the Norwegian oversight committee); Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 24 (as amended); Norway, Instructions for Monitoring of Intelligence, Surveillance and Security Services (EOS), Issued pursuant to section 1 of Act No. 7 of 3 February 1995 relating to the Monitoring of Intelligence, Surveillance and Security Services, Section 8; New Zealand, Inspector-General of Intelligence and Security Act (1 July 1996), Section 25; Kenya, National Security Intelligence Service Act (31 December 1998), Section 26.
64. United Kingdom, Investigatory Powers Tribunal web site, "Complaints process: What happens to my complaint?" (http://www.ipt-uk.com/sections.asp?sectionID=4&chapter=0&type=top); United Kingdom, Regulation of Investigatory Powers Act 2000, Chapter 23, Section 67.
65. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the National Security Activities* (2006), p. 18.

List of Contributors

HANS BORN is a senior fellow at DCAF. He currently focuses on intelligence oversight as well as the role of parliaments and ombuds-institutions in security sector governance. His regional specialization is Southeast Asia (including Cambodia, Indonesia, the Philippines and Thailand). He has conducted policy research studies in the areas of human rights, accountability and security sector governance for the United Nations, the Organisation for Security and Co-operation in Europe, the Council of Europe and the European Parliament. He co-initiated the Inter-Parliamentary Forum for Security Sector Governance in Southeast Asia (www.ipf-ssg-sea.net) and the International Conference for Ombuds-Institutions for Armed Forces (www.icoaf.org). He has published widely on security sector reform and governance. His latest publications include *Governing the Bomb: Democratic accountability and civilian control of nuclear weapons* (Oxford University Press, 2011), *Accountability of International Intelligence Cooperation* (Routledge 2011) and *Parliamentary Oversight of the Security Sector: ECOWAS Parliament-DCAF Guide for West African Parliamentarians* (ECOWAS, 2011). He holds an MA in Public Administration from the University of Twente and a Ph.D. in social sciences from Tilburg University (the Netherlands).

AIDAN WILLS is a project coordinator in DCAF's Research Division, where he has worked on security and intelligence governance for six years. He was the lead consultant in drafting the UN compilation of good practices on intelligence services and their oversight. More recently, Aidan co-authored a major European Parliament study on *Parliamentary Oversight of Security and Intelligence Services in the European Union*, and co-edited a volume on *International Intelligence Cooperation and Accountability*. He has delivered training to intelligence and security oversight bodies throughout Europe and the Middle East, and has also contributed to various legislative processes. Aidan has acted as a consultant to the Council of Europe, European Parliament and the UN Special Rapporteur (on human rights and counter terrorism) on various aspects of security sector governance and human rights. He is currently involved in the Open Society Foundation-led development of a compilation of *Global Principles on National Security and the Right to Information*.

MONICA DEN BOER holds a position at the Police Academy of the Netherlands and is a member of the Committee on European Integration of the Advisory Council on International Affairs. She obtained a Ph.D. in 1990 from the European University Institute and worked at Edinburgh University, the Netherlands Study Centre for Crime and Law Enforcement, the European Institute of Public Administration, Tilburg University, and the European

Institute of Law Enforcement Co-operation. Between March 2004 and January 2012 she was professor of comparative public administration at the VU University Amsterdam on behalf of the Police Academy of the Netherlands. In 2009, she was a member of the Dutch Iraq Investigation Committee, and in 2009-2010 she participated in the Defence Future Survey Group. She has published widely on European internal security co-operation and engages in teaching, coaching as well as supervision.

STUART FARSON is an adjunct professor of political science at Simon Fraser University. In 1989-90 he served as research director for the first and only statutory parliamentary review of the Canadian Security Intelligence Service Act. He was an expert witness for the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. More recently he co-authored with Reg Whitaker "Accountability in and for National Security," IRPP Choices (2009). He also co-edited Commissions of Inquiry and National Security (2011) and the PSI Handbook of Global Security and Intelligence: National Approaches (2008), both published by Praeger.

CRAIG FORCESE is a vice dean and associate professor at the Faculty of Law (Common Law Section), University of Ottawa. He teaches public international law, national security law, administrative law and public law/legislation. Much of his present research and writing relates to national security, human rights and democratic accountability. Craig is currently president of the Canadian Council on International Law. He is the author of, among other things, *National Security Law: Canadian Practice in International Perspective* (Irwin Law, 2008) and co-editor of *Human Rights and Anti-terrorism* (Irwin Law, 2008).

GABRIEL GEISLER MESEVAGE is a doctoral candidate at the Graduate Institute of International and Development Studies where he also works as a teaching assistant. He has also worked as a research assistant at the Graduate Institute, studying corruption in the private sector. From 2010-2011, Gabriel worked at DCAF in the Research Division, where his research focused on the governance of police and intelligence services. During his time at DCAF, Gabriel contributed to the external oversight section of the DCAF *Toolkit on Police Integrity*. He holds an MA First Class Honours in International Relations and Social Anthropology from the University of St Andrews and an MA in International Studies from the Graduate Institute of International and Development Studies.

LAUREN HUTTON has been working as a researcher and practitioner on security sector reform and post-conflict transformation in Africa since 2005. She currently works as an advisor for the Danish Demining Group and the Danish Refugee Council in South Sudan, focusing on conflict sensitivity and armed violence reduction. Lauren previously worked for Saferworld and the Institute for Security Studies (ISS). While at the ISS, Lauren developed a project on the democratic governance of intelligence in Africa. Through this, she provided input into the 2007 intelligence review process and legislation drafting processes in 2009 and 2010 in South Africa, and provided training to parliamentarians in southern and eastern Africa on intelligence oversight. She also edited a volume on intelligence and democracy in South Africa, *To spy or not to spy*, and published several journal articles and occasional papers on intelligence governance during this time. Lauren holds a Master's Degree in Political Studies from the University of the Western Cape (South Africa).

IAN LEIGH is professor of law at Durham University and is a member of the Durham Global Security Institute. His books include *In From the Cold: National Security and Parliamentary Democracy* (Oxford University Press, 1994), with Laurence Lustgarten, *Who's Watching the*

Spies: Establishing Intelligence Service Accountability (Potomac Books, 2005) with Hans Born and Loch Johnson, and *International Intelligence Cooperation and Accountability* (Routledge, 2011), with Hans Born and Aidan Wills. His policy report *Making Intelligence Accountable* (with Dr Hans Born, published by the Norwegian Parliament Printing House 2005) has been translated into 14 languages. He has also co-authored the *OSCE/DCAF Handbook on Human Rights and Fundamental Freedoms of Armed Forces Personnel* (Warsaw, 2008) and has acted as a consultant to the OSCE Office of Democratic Institutions and Human Rights, to the Venice Commission on democratic control of security and intelligence agencies in Council of Europe states, and to the UNDP on security sector reform.

LAURIE NATHAN is extraordinary professor and director of the Centre for Mediation at the University of Pretoria. He is a visiting professor at Cranfield University, where he teaches a Master's course on intelligence reform. His most recent book is *Community of Insecurity: SADC's Struggle for Peace and Security in Southern Africa, Ashgate* (2012). He served on the Ministerial Review Commission on Intelligence in South Africa (2006-8) and drafted South Africa's White Paper on Defence (1996). He has been a member of the Advisory Committee of the Arms Division of Human Rights Watch; the Carter Center's International Council for Conflict Resolution; and the Expert Advisory Group of the UNDP Democratic Governance Practice Network. He is a member of the UN Mediation Roster and the UN Roster of SSR Experts.

KENT ROACH is a professor of law at the University of Toronto where he holds the Prichard Wilson Chair in Law and Public Policy. He was a member of the research advisory committee of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar and was research director of the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182. His most recent book is *The 9/11 Effect: Comparative Counter-Terrorism*, published by Cambridge in 2011.

BERT VAN DELDEN joined the Dutch judiciary in 1966. He was president of the District Court of The Hague from 1990- 2001 and was then appointed as the first chair of the Council for the Judiciary. After his retirement from the judiciary he was appointed as a member of the Dutch Review Committee for the Intelligence and Security Services (CTIVD). Since 2009, he has served as the chair of this committee.

THEODOR H. WINKLER has been director of the Geneva Centre for the Democratic Control of Armed Forces (DCAF) since 2000, when the Swiss Federal Council promoted him to the rank of ambassador and appointed him to head the newly-created centre. He joined the Swiss Department of Defence in late 1981 as an international security expert. In 1985 he was appointed representative of the chief of staff for politico-military affairs, and in 1995 he became head of the newly-created Division for International Security Policy. He was subsequently promoted to the rank of deputy head, security and defence policy. Winkler studied political science and international security at the University of Geneva, Harvard University and the Graduate Institute of International Studies - Geneva. In 1981 he obtained a Ph.D. in political science with a thesis on nuclear proliferation.

Overseeing Intelligence Services

A Toolkit

This toolkit is a compendium of booklets written by leading experts on intelligence governance from around the world. It provides policy-relevant guidance on the establishment and consolidation of intelligence oversight systems, as well as on the oversight of specific areas of intelligence services' work including: the collection of information, the use of personal data, information sharing with domestic and foreign partners, and their finances. This guidance is based on legal and institutional frameworks and practices from numerous states.

While the toolkit focuses on parliamentary and independent oversight bodies, it contains numerous insights that are relevant to the executive, judiciary, media, civil society and intelligence services themselves. This toolkit is likely to be of particular interest to members and staffers of oversight bodies; actors involved in monitoring the work of overseers (e.g., the media, civil society organisations and parliamentarians); and to the subjects of external oversight: the executive branch and intelligence services.

The Geneva Centre for the Democratic Control of Armed Forces (DCAF) is an international foundation whose mission is to assist the international community in pursuing good governance and reform of the security sector. The Centre develops and promotes norms and standards, conducts tailored policy research, identifies good practices and recommendations to promote democratic security sector governance, and provides in-country advisory support and practical assistance programmes.

www.dcaf.ch