Making International Intelligence Cooperation Accountable

Hans Born, Ian Leigh, Aidan Wills

EOS COMMITTEE
NORWEGIAN PARLIAMENTARY OVERSIGHT COMMITTEE
ON INTELLIGENCE AND SECURITY SERVICES

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

Making International Intelligence Cooperation Accountable

Hans Born, Ian Leigh, Aidan Wills

EOS COMMITTEE
NORWEGIAN PARLIAMENTARY OVERSIGHT COMMITTEE
ON INTELLIGENCE AND SECURITY SERVICES

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

Authors: Hans Born, Ian Leigh and Aidan Wills

Editorial assistants: Youngchan Kim and William McDermott

Designer: Alice Lake-Hammond

Cover photograph: Tobias Schwarz/AFP/Getty Images
Cover photograph description: German intelligence service (BND) chief Gerhard Schindler arrives at the enquiry commission of the German Bundestag on the US intelligence agency NSA in Berlin, on 21 May 2015

Background cover image: polygraphus/Shutterstock.com

This publication has been made possible by the generous support of the Norwegian Parliamentary Intelligence Oversight Committee.

Published by: Printing Office of the Parliament of Norway

ISBN: 978-92-9222-375-5

Contents

List of Boxes

List of Acronyms

ACHPR – African Commission on Human and Peoples' Rights

AIVD – General Intelligence and Security Service of the Netherlands

ALD – Administrative Law Decisions (Australia)

ARSIWA – Articles on Responsibility of States for Internationally Wrongful Acts

ASIO – Australian Security Intelligence Organisation

AU – African Union

BfV – *Bundesamt für Verfassungsschutz* (Federal Office for the Protection of the Constitution - Germany's domestic intelligence service)

BND – *Bundesnachrichtendienst* (Germany's foreign intelligence service)

CAT – Convention Against Torture

CdB – Club of Berne

CMP – Closed Material Procedures

CIDT – cruel, inhuman and degrading treatment

CISSA – Committee of Intelligence and Security Services of Africa

CIA – Central Intelligence Agency (US)

COMSEC – communications security

CSE – Communications Security Establishment (Canada)

CSIS – Canadian Security Intelligence Service

CTIVD - Review Committee on the Intelligence and Security Services (the Netherlands)

CUTA – Coordination Unit for Threat Analysis (Belgium)

DCAF – Geneva Centre for the Democratic Control of Armed Forces

DCRI – *Direction Centrale du Renseignement Intérieur* (France)

DDIS – Danish Defense Information Service

DGSE – *Direction générale de la sécurité extérieure* (France's foreign intelligence service)

DIA – Defense Intelligence Agency (US)

DISS – Defence Intelligence and Security Service (the Netherlands)

DNI – Director of National Intelligence (US)

ECHR – European Convention on Human Rights

ECtHR – European Court of Human Rights

EOS Committee – Norwegian Parliamentary Oversight Committee on Intelligence and Security Services

EC – European Community

EP – European Parliament

EU – European Union

EUROPOL – European Union Police Office

EYP-NIS – National Intelligence Service (Greece)

FBI – Federal Bureau of Investigation (US)

GCHQ – Government Communications Headquarters (UK)

GCSB – Government Communications Security Bureau (New Zealand)

GISS – General Intelligence and Security Service (the Netherlands)

HQ - Headquarters

HR – Human rights

HRC – Human Rights Council

HUMINT – Human intelligence

ICCPR – International Covenant on Civil and Political Rights

ICTY – International Criminal Tribunal for the Former Yugoslavia

IIC – international intelligence cooperation

IGIS – Inspector General of Intelligence and Security (Australia)

IHL – International Humanitarian Law

ILC – International Law Commission

INTCEN – Intelligence Analysis Centre (EU)

IO – international organisation

IPT – Investigatory Powers Tribunal (UK)

IRA – Irish Republican Army

IS – Islamic State in Iraq and Syria

ISC – Intelligence and Security Committee (UK)

ISNU – Israeli Signals Intelligence National Unit

JTAC – Joint Terrorism Analysis Centre (UK)

LIBE – Committee on Civil liberties, Justice and Home Affairs (European Parliament)

MoU – memorandum of understanding

NATO – North Atlantic Treaty Organisation

NGO – non-governmental organisation

NIA – National Intelligence Agency (South Africa)

NIS – Norwegian Intelligence Service

NSA – National Security Agency (US)

NZ – New Zealand

NZSIS – New Zealand Security Intelligence Service

OAS – Organization of American States

OSCE – Organization for Security and Cooperation in Europe

PACE – Parliamentary Assembly of the Council of Europe

PST – Police Security Service (Norway)

RCMP – Royal Canadian Mounted Police

SAI – Supreme Audit Institutions

SGRS – *Service général de renseignement et de la sécurité* (Belgium)

SIGINT – Signals intelligence

SIS – Secret Intelligence Service (UK)

SIRC – Security Intelligence Review Committee (Canada)

SREL – *Service de renseignement de l'Etat Luxembourgeois*

TDIP – Temporary Committee on the alleged use of European countries by the CIA for the transport and illegal detention of prisoners

UK – United Kingdom

UKUSA – United Kingdom – United States of America Agreement, also known as Five Eyes

UN – United Nations

UNSC – United Nations Security Council

US – United States

USSR – Union of Soviet Socialist Republics

UPR – Universal Periodic Review

WMD – weapons of mass destruction

WW2 – World War Two

Foreword

International cooperation across state borders is crucial to intelligence services in their work to detect and prevent threats to free and open societies. In our days, the need for international intelligence cooperation is particularly apparent through intelligence service's work against international terrorism. As movements of people in and out of instable, volatile regions of the world increases, and organisations like Al Qaeda and the Islamic State (IS) in Iraq and Syria have taken root, the need for trans-border cooperation has grown. Nevertheless, just as increased intelligence cooperation might be a necessity, and intelligence services are put under pressure by the public to detect and prevent acts of terror, there is a stronger need for democratic oversight.

This book examines accountability in intelligence cooperation from several perspectives. The study is useful to oversight bodies, intelligence services themselves, as well as to the general public. First, it gives an update on nature of and the areas and landscapes in which intelligence cooperation takes place. In this respect, not only are benefits and risks reviewed, but also practical and ethical dimensions are discussed. Second, through addressing domestic and international legal standards pertaining to intelligence cooperation, the book gives a much needed update on key legal aspects of such cooperation. Third, as there is no "one size fits all" solution to oversight, the part of the book on the implementation of accountability and democratic control in practice is of particular relevance to overseers. In this part, the merits of both internal mechanisms, as

well as external oversight bodies are presented, giving the reader a holistic approach to how institutional arrangements can contribute to accountability.

Finally, while modern democratic states need the products and services provided by intelligence organizations, their growing sophistication and expanding reach, given technological developments, make oversight more relevant than ever. Against this background, on behalf of the Norwegian Parliamentary Intelligence Oversight Committee, I welcome this book, as a highly insightful and relevant contribution to an important topic that should be debated in the years to come.

Eldbjørg Løwer
Chair, Norwegian Parliamentary Oversight Committee on Intelligence and Security Services
Oslo, 3 September 2015

Acknowledgements

This guide is a sequel to the 2005 report *Making Intelligence Accountable*, which dealt with the topic of best practices for oversight of security and intelligence services. When that study was completed, concerns about the effectiveness of oversight bodies in handling the international cooperation activities of the services that they oversee were already emerging. In the ensuing decade they have steadily accumulated. When we first conceived the idea of a second policy study focused on accountability and international cooperation in 2007, there was a paucity of available public material. We are grateful for the far-sighted support and encouragement of the Norwegian Parliamentary Intelligence Oversight Committee who agreed once again to partner the project and to host an international conference in Oslo in 2008 on a topic that was at that time somewhat speculative. A number of papers from the conference were published, including *International Intelligence Cooperation and Accountability* in 2011.[1] We are grateful to all contributors and participants for helping to develop our thinking. The edited volume is an academic companion study to this policy guide.

When it came to turn the academic analysis into developing the policy guide, we were fortunate in being able to draw on the insights of numerous former senior intelligence officials and current and former oversight practitioners from three continents, who generously agreed to be interviewed on condition of anonymity. We would like to express our gratitude to all of those who shared their knowledge and experience with us – your contribution has greatly enriched this guide.

In addition, we were also exceptionally fortunate in enlisting an international advisory board composed of former senior intelligence officials, overseers and academic specialists. Members of the advisory board commented extensively on an early draft and directed us towards additional material. Several members of the board also took part in a review workshop in Geneva in 2013 from which we were able to gain insights into the nature of international intelligence cooperation, the benefits it brings and the feasibility of solutions to the challenges that arise in and from this cooperation.

We would like thank the following people for contributing to the advisory board in their personal capacity: Hazel Blears (former Member of Parliament and its Intelligence and Security Committee, United Kingdom), Barry Gilder (former Coordinator of Intelligence and Director-General of Department of Home Affairs, South Africa), Philippe Hayez (former Deputy Director for Collection and Analysis at the Directorate General for External Security, DGSE, France), Liesbeth Horstink (Member of the Review Committee on the Intelligence and Security Services, The Netherlands), Jantine Kervel (Member of staff of the Review Committee on the Intelligence and Security Services, The Netherlands), Theo Koritzinsky (Member of the Norwegian Parliamentary Intelligence Oversight Committee), David Omand (former Director of GCHQ and former Security and Intelligence Coordinator, United Kingdom), Kent Roach (Professor of Law and Prichard-Wilson Chair of Law and Public Policy at the University of Toronto Faculty of Law, Canada), Andrej Rupnik (former Director of National Intelligence and Security Agency, Slovenia), Günther Schirmer (Deputy Head of Secretariat, Committee on Legal Affairs and Human Rights, Parliamentary Assembly of the Council of Europe, Strasbourg), Cyrille Fijnaut (Professor of Law at the Faculty of Law at Tilburg University, the Netherlands).

We should stress, however, that liability for the contents of this guide is with the authors alone and no member of the advisory board has approved or is in any way responsible for the contents. While the guide is the collective responsibility of the authors, Hans Born took the lead on chapters 1, Ian Leigh on chapters 4, 5 and 8, and Aidan Wills on chapters 2, 3, 6 and 7.

By the time we completed the study, the initial trickle of information about international intelligence cooperation had become something of a flood, due to successive revelations about and inquiries into rendition, black sites and mass surveillance. The accumulating body of material has delayed the study but has, we hope, led to a stronger and better-informed final product. We are grateful for the unfailing support throughout the whole

process of the Norwegian Parliamentary Intelligence Oversight Committee Chair Eldbjørg Løwer (as well as her predecessor Helga Hernes), Henrik Magnusson (Head of Committee Secretariat), Njord Wegge (Senior Political Advisor) and other members of the staff.

We have also been ably assisted by the following colleagues at DCAF, Nargiz Arupova, Youngchan Kim, and Will McDermott.

Hans Born, Geneva
Ian Leigh, Durham
Aidan Wills, London

August 2015

1. Hans Born, Ian Leigh and Aidan Wills, ed., *International Intelligence Cooperation and Accountability*, (London: Routledge, 2011).

1

Introduction

Intelligence services perform a valuable service to democratic society in protecting national security, including the protection of fundamental freedoms and human rights of all individuals. Because intelligence services work clandestinely and the nature of their task often requires them to fulfil their work in secret, they are at odds with the principle of an open society. The secret nature of intelligence work applies in particular to international cooperation, where intelligence services try to keep secret why, how, and when they cooperate with other states. Against this background, accountability of international intelligence cooperation may sound like a contradiction in terms. Indeed, accountability requires transparency, while intelligence services require secrecy. In spite of these contradictory requirements, many states have found solutions for applying accountability to the secret world of international intelligence cooperation. In this guide, on the basis of an analysis of legal and institutional frameworks and the identification of good practices of international intelligence cooperation, we will explore how states have reconciled the need for accountability and transparency with the operational need for secrecy, allowing intelligence services to conduct their operations successfully.

In this introductory chapter, a brief overview will be given of the aims, scope, target audience, and methodology of the guide on accountability of international intelligence cooperation.

1.1 Relevance of the guide

The development of a guide on accountability of international cooperation is a challenging but important undertaking. At least four reasons make this guide relevant for overseers and other interested parties: (1) the significant and ongoing increase in the breadth and depth of international intelligence cooperation, (2) the need to provide overseers with a practical guide on how they can go about holding intelligence services and the executive to account for international intelligence cooperation; (3) to assess how the risks of international intelligence cooperation, in particular risks for human rights and the rule of law, can be addressed through accountability; and (4) to provide guidance on the legal framework under which international intelligence cooperation occurs.

A first reason is that international cooperation has become a much more important part of the work of intelligence services and most, if not all, functions of intelligence services include an international dimension. Indeed, the rapid pace of globalisation has contributed to the expansion of the scope and scale of international networks engaged in threats to national security, serious organized crime, terrorism, and the proliferation of weapons of mass destruction. The growth of these transnational threats has resulted in an increase of international intelligence cooperation in order to keep up with these threats to national and regional security. While international intelligence cooperation (IIC) has existed for centuries, the responses of states and international organisations to 9/11 have exponentially increased the scope and scale of intelligence cooperation, in particular between Western states and non-traditional partners. International organisations, notably the UN Security Council, have expressly encouraged or even mandated the sharing of intelligence on terrorism between states. Moreover, the threats posed by terrorist and militant groups of varied nature continue to demonstrate that international intelligence cooperation is necessary. These threats cannot be contained by one state alone and require an internationally coordinated response. For example, in the case of Boko Haram, the United States increased its intelligence cooperation with Nigeria and neighbouring states to aid efforts to locate and free hostages.[1] Similarly, in the case of the so-called Islamic State (IS) in Iraq and Syria, for example, UN Security Council Resolution 2178 calls upon states to improve international cooperation, including the increased sharing of information with the purpose of identifying "international terrorist fighters."[2] Once again, in response to threats posed by the terrorist group Al Shabaab based in Somalia, intelligence agencies of states in East Africa and Western states have increased their intelligence cooperation.[3] These and other current examples underline the increased importance of international intelligence cooperation and, therefore, equally underscore the increased importance of how oversight bodies can hold services accountable for their international cooperation.

The growing importance of cooperation emphasises the second reason why this guide has been drafted: to fulfil an increasing need for specific guidance on how accountability and oversight of international intelligence cooperation can be strengthened on the basis of practical examples. Indeed, international intelligence cooperation is a challenging subject for overseers, and various characteristics of international intelligence cooperation can in some respects threaten or undermine the accountability processes. Arguably the greatest threat to accountability in this area is the third party rule which forms one of the pillars of

international cooperation. The third party rule, also known as the principle of "originator control" prescribes that information shared with foreign services cannot be shared with third parties without permission of the service that supplied the information. Usually, oversight bodies are considered to be third parties and, for that reason, intelligence services are reluctant to share information related to international cooperation with their overseers. Another major challenge is that international intelligence cooperation involves two or more different jurisdictions whereas oversight bodies are creatures of domestic law. Parliamentary or expert oversight bodies do not have the legal power to therefore compel intelligence officials of other states to attend hearings or to cooperate in their inquiries.

A third rationale of the guide is that some aspects of international intelligence cooperation have given rise to serious concerns over the past decade. A series of scandals and accusations of wrongdoing have been made related to the part that international intelligence cooperation has played in the abduction and secret detention of suspects, abusive interrogation techniques, extraordinary rendition of suspects to states with dubious human rights records, as well as mass surveillance as revealed by the Snowden leaks. These alleged wrongdoings show that international intelligence cooperation is a high-risk area of state activity and thus requires an effective legal framework and oversight. Accountability can help not only in countering the risks of international intelligence cooperation but also in realizing its potential benefits. Effective cooperation has become critical for the success of intelligence work. Consequently, accountability must ensure that intelligence services have the proper mandate, resources and legal framework to cooperate with services of other countries. Rather than juxtaposing accountability versus international intelligence cooperation, the focus should be how accountability can contribute to successful international intelligence cooperation within the boundaries of the law and with respect for human rights.

A fourth reason for producing this publication is to provide guidance on the relevance of international law and how the domestic legal framework governing international intelligence cooperation can be improved. Intelligence has become increasingly legalised in the past 30 years. Most democratic states have departed from the old habit of establishing their intelligence services under (secret) executive decrees and have decided instead to base their services on statutory publicly available law, enacted by parliament. However, this process of legalisation has yet to be fully extended to international intelligence cooperation. In many states, including democratic states, the laws governing the intelligence services do not include provisions on either the conditions for cooperation or on the mechanisms for its authorisation and oversight.[4] This guide provides practical examples on how intelligence laws can be improved through incorporating provisions on international cooperation and its oversight.

1.2 Aims of the guide

Against this backdrop, international intelligence cooperation and its oversight has become much more important during the last decade and nothing that is written in this guide should be interpreted as indicating that such cooperation should not take place or should not continue to expand as necessary to address threats to national security. However, international intelligence cooperation – including information sharing as its most prominent form - has the potential to infringe upon human rights. As Judge Dennis O'Connor stated in the Arar inquiry report (see Box 3.3 in Chapter 3 for more information), intelligence cooperation with other countries can cause a "ripple effect" beyond the country's borders with consequences that may not be controllable from within the country.[5] In this context, the guide seeks to provide practical and specific guidance on how accountability and oversight of international intelligence cooperation can be strengthened on the basis of practical examples. Specifically, this guide has four aims.

First, the aim of the guide is to provide practical guidance on how the potential implications of international intelligence cooperation can be assessed and, where appropriate, on how the decisions involved in cooperation can be based on legislation and made accountable. Helping overseers in the executive, parliament, and in expert oversight bodies to grapple with these very complex and sensitive issues is a preeminent aim of this guide. Furthermore, the guide aims to support relevant parties in establishing or reforming a legal framework to improve accountability and human rights compliance for international intelligence cooperation.

Second, the guide intends to highlight the roles and responsibilities of the various state institutions involved in international intelligence oversight and its oversight. These institutions include internal management of the services, executive, parliament, and the judiciary, as well as expert intelligence oversight bodies.

A **third** aim of this guide is to contribute to an informed debate about the challenges, scope, and limits of holding intelligence services accountable for their conduct of international cooperation. Intelligence overseers seem to experience international intelligence cooperation as a challenging area of work. For example, Helga Hernes, former chair of the Norwegian Parliamentary Intelligence Oversight Committee, has stated that international intelligence cooperation is a challenging area of work for oversight bodies because information coming from partner services "is traditionally regarded as particularly sensitive, and national oversight bodies are usually obliged to show restraint in asking access to such material, or they are totally cut off."[6] One has to bear in mind that this assessment comes from Norway, where intelligence activities are extensively regulated and systematically overseen by an independent oversight body with formidable powers and resources. One can only imagine the challenges to the accountability of international intelligence cooperation in states with an undeveloped or under-resourced oversight system. Therefore, the guide aims to raise awareness of the challenges for accountability inherent in international intelligence cooperation and how these challenges can be addressed.

The **fourth** aim of this guide is to identify good practices and lessons learned from existing models for oversight of international intelligence cooperation. Various states have subjected international intelligence cooperation to a system of extensive internal and external oversight. Therefore, this guide not only aims at mapping the challenges and risks of international intelligence cooperation, but also to deal with the policies, practices, and experiences related to holding intelligence services to account for their international cooperation activities.

1.3 How little we know[7]

Until relatively recently, international intelligence cooperation was a black box about which states gave very little or no information and which was not covered by academic research. The secrecy surrounding international cooperation was so high that it was thought to be impossible to address issues of accountability. Because international cooperation is among the most jealously guarded and sensitive areas of intelligence activity, it is shrouded in secrecy, and a lack of information exists among overseers, let alone among members of the public. The paucity of information is exacerbated by the third party rule which shields the information obtained from partner services of other countries from attribution. Many laws on intelligence services or on freedom of information contain exemptions that prevent disclosure not only to the public but also to intelligence oversight bodies, who are often considered to be third parties.

This blackout of publicly available information about international intelligence cooperation has slightly changed in the last decade for at least two reasons. First, triggered by reports in the media in the years after 9/11, parliamentary, expert intelligence oversight bodies, and *ad hoc* inquiries have investigated and published details of numerous high profile controversies involving international intelligence cooperation. These investigations especially dealt with extraordinary rendition and secret prisons in Europe, and in this guide we will cover some of these investigations.[8]

Second, the revelations of Edward Snowden in 2013 not only disclosed the extent of mass surveillance conducted by intelligence services but also revealed the extent of international cooperation between services in the area of signals intelligence (SIGINT). These revelations prompted numerous parliamentary, expert intelligence oversight bodies, and *ad hoc* inquiry committees to investigate the surveillance powers of their intelligence services and whether services have complied with the rule of law and respected human rights while cooperating with services of other states. These investigations, both at the national and international levels, have covered international cooperation aspects as part of their investigations into the Snowden leaks. At the international level, these include the inquiry of the European Parliament's LIBE Committee on mass surveillance of citizens of EU member states (2013-2014),[9] the Parliamentary Assembly of the Council of Europe report on mass surveillance in 2015,[10] the report of the Venice Commission of the Council of Europe in 2015 on democratic control of signals intelligence agencies,[11] as well as the expert study on democratic oversight of intelligence services commissioned by the Council of Europe Human Rights Commissioner in 2015.[12] At the national level, various parliamentary

and expert oversight bodies have started investigations into the Snowden leaks and these investigations have invariably included elements of international cooperation. For example, the Belgian Standing Intelligence Review Committee commissioned two expert-studies on the Snowden revelations in relation to the PRISM programme.[13] Similarly, the Intelligence and Security Committee of the UK Parliament took into account the international cooperation dimension while assessing the legal framework of intelligence services in 2015.[14] Elsewhere, in the wake of the Snowden leaks, the Dutch Review Committee for Intelligence and Security Services is currently investigating the criteria and ministerial authorisation processes of international intelligence cooperation.[15] In Germany, the Bundestag Committee of Inquiry into the "NSA affair" was established on 20 March 2014 on request of all parliamentary factions, and it was mandated to investigate international intelligence cooperation activities in Germany and to what extent German authorities and intelligence services were involved and/or had prior knowledge.[16]

1.4 What this guide will cover

As will be detailed in the next chapter, this guide defines *international intelligence cooperation* as the liaison or collaboration between state bodies responsible for the collection, analysis and/or dissemination of information in the field of national security and defence.[17] Such cooperation is undertaken by military and civilian intelligence services, in the form of stand-alone services, as well as constituent units of ministries or armed forces, whose mandates may be domestic and/or foreign, and, in some states, by the intelligence branches of national police services. The guide is limited to cross-border/international cooperation between state institutions with a mandate to protect national security. Therefore, this guide will not deal with international intelligence cooperation undertaken by or involving private/non-state organisations or cross-border law enforcement cooperation and mutual legal assistance.

As the guide deals with *accountability* of international intelligence cooperation, it is necessary to unpack this concept and to relate it to associated concepts. In this context, we will use a family of concepts including accountability, oversight and control.

Oversight is a catchall term that refers to scrutinising the work of intelligence services and its officers with the aim of assessing compliance with specific criteria and, on the basis of this, to issue recommendations or even orders to intelligence services and its responsible minister. Oversight can occur at several different points in time. If oversight occurs at the outset of an activity related to international cooperation that has been proposed but not yet undertaken, then it is called *ex ante* oversight. Furthermore, oversight can take place while an activity is under way (ongoing oversight), or it can occur after the activity has concluded (*ex post* oversight).[18]

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 in international intelligence cooperation, such as counterterrorism. Readers should be aware, however, that not every national system of intelligence oversight makes a clear distinction between oversight and control. For this reason, some institutions described in this publication 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. The term *accountability* is central to this publication and it carries multiple meanings and uses. At the most basic level, accountability is best understood as a process of account giving and account holding that takes place within an established relationship. In this relationship, the intelligence service (or individual within the service) is the account giver, who can be obligated to render account to the overseer, which has the right to demand such account. Accountability has four components: 1) the intelligence services or its individual officers that are held to account; 2) the institution to which they give account (overseer); 3) the areas of intelligence work that are subject to accountability; and 4) the legal, financial, resource, and expert capacity of the overseer to hold intelligence services accountable for international intelligence cooperation.[19]

Box 1.1, below, gives an overview of *overseers* who are involved in accountability of international intelligence cooperation and who will be addressed in this guide, including their possible oversight responsibilities. While the important role of civil society and media is acknowledged in this guide, for example, in triggering official inquiries into international intelligence cooperation, they are not especially addressed, as this guide focuses on state bodies. Readers are advised that the responsibilities of overseers are managed differently in different states, and the oversight system of a particular state may not address all of the responsibilities identified in the Box 1.1.

Whether accountability or oversight can be qualified as *democratic accountability* or *democratic oversight* depends on whether these activities are conducted by democratically elected individuals instead of appointed individuals, for example, an elected member of parliament or of the executive. Furthermore, it can only be called democratic if those elected individuals themselves give account of their oversight activities in a transparent way, in accordance with the rule of law and with respect for human rights. On this note, intelligence services benefit from democratic accountability because democratic accountability binds both the intelligence services and their political masters. Therefore, accountability mechanisms help to protect the services from abuse by their political leaders and from ill-informed media speculation. Furthermore, if international intelligence cooperation is subjected to clear authorisation and monitoring procedures which are based on the law enacted by parliament, it may help to ensure that these activities have greater legitimacy in the eyes of the people and their representatives in government and parliament.

Box 1.1: Overview of selected possible oversight responsibilities related to international intelligence cooperation

OVERSIGHT BODIES	SELECTED POSSIBLE KEY RESPONSIBILITIES
Senior management of the services	▪ Setting international intelligence cooperation requirements within the broader intelligence and security priorities ▪ Developing internal guidelines on the scope, authorization, tasking, and monitoring procedures related to international intelligence cooperation ▪ Reporting to ministers on intelligence relations with other states ▪ Conducting assessments of services of new partner states
Executive (ministers)	▪ Coordinating international intelligence cooperation with foreign and national security policy ▪ Approving important new, intensifying, or discontinuation of relationships ▪ Deciding on the policy framework and setting general parameters on the types of relationships and cooperation allowed, and the process for authorization, implementation, and monitoring ▪ Approving of individual sensitive and high risk international cooperation activities in accordance with national legislation
Parliament (and parliamentary oversight bodies)	▪ Initiating, amending, or updating the legal framework pertaining to international intelligence cooperation (law-making function) ▪ Scrutinising activities related to international intelligence cooperation (oversight function) ▪ Approving, rejecting, or amending the budget of intelligence services, including international intelligence cooperation (budget functions)
Expert oversight bodies	▪ Advising parliament and/or the executive on laws that pertain to international intelligence cooperation and assuring that it is sufficiently covered by law ▪ Overseeing the propriety, legality, effectiveness, and efficiency of international intelligence cooperation ▪ Investigating issues related to international intelligence cooperation
Judiciary	▪ Authorizing *ex ante*, where laid down in legislation, and/or reviewing *ex post* the use of special powers in the context of international cooperation ▪ Adjudicating criminal, civil, constitutional, and administrative law cases that concern international intelligence cooperation ▪ Advising expert bodies and conducting at the request of government *ad hoc* inquiries into international intelligence cooperation

This guide will also pay attention to the primary constraint on oversight of international intelligence cooperation, i.e. that it should not impair protection of national security.[20] This implies that overseers should respect the professional judgments and assessments of the services (insofar within the scope of the law), understand the importance of secrecy, and will protect classified information to which they have access as part of their role. The acknowledgement of the rather fine line between effective and excessive oversight is one of the considerations of the conceptualization and drafting of the guide.

1.5 Target audience

This guide is written for anyone who is interested in or concerned with the challenges and possibilities for the accountability of international intelligence cooperation. These interested or concerned parties can be found, firstly, within the parliamentary and expert oversight bodies, as well as the judiciary. Secondly, the guide will be of interest to those within the executive who are responsible for the conduct of intelligence services, including ministers and their civil servants in ministries of home affairs, defence and foreign affairs. Thirdly, the guide will be of interest for those within the services who are responsible for the policy, guidelines/rule books, priorities, authorisation, monitoring, and coordination of international intelligence cooperation. These include heads of services, managers, legal advisors, and those working in the training units of the services. Fourthly, the guide is of relevance for those working in international organisations (e.g. United Nations (UN) or the North Atlantic Treaty Organisation – NATO), who are involved or concerned with international intelligence cooperation. Last but not least, the guide may be of interest for the members of the general public, including civil society organisations, advocacy organisations, academia, or the media.

1.6 Structure of the guide

The guide will start by outlining the scope and nature of the international intelligence cooperation in Chapter 2. This chapter discusses the rationale and drivers of international intelligence cooperation, different forms and modes of cooperation, and recent trends. This will be followed by an analysis of the benefits and risks of international cooperation (Chapter 3). These two chapters form together Part I, "International Intelligence Cooperation."

This is followed by two chapters dealing with the "Legal Frameworks of International Intelligence Cooperation" (Part II). Part II starts with Chapter 4 addressing the international legal standards for international cooperation and is followed by Chapter 5 on the review of domestic legal frameworks regulating international intelligence cooperation. Part III "Accountability of International Intelligence Cooperation" deals with the implications for different categories of overseers. Chapter 6 focuses on the internal controls within the services as well as the role of the role of the executive in overseeing international intelligence cooperation. Chapter 7 deals with parliamentary and expert intelligence oversight bodies, as well as *ad hoc* inquiry committees. Finally, Chapter 8 addresses the role of the courts in international intelligence cooperation.

1.7 Methodology

This guide is written with support of the Norwegian Parliamentary Oversight Committee on Intelligence and Security Services (EOS Committee)[21] and is part of a multi-year project on the accountability of international intelligence cooperation, started in 2008. The guide builds upon a small body of literature on the oversight of international intelligence

cooperation, in particular the edited volume "International Intelligence Cooperation and Accountability,"[22] which was part of the aforementioned project. Furthermore, the guide is based on more than a dozen interviews with current and former intelligence overseers, intelligence officials, and independent experts based in North America, Europe, and Africa, who agreed to be interviewed on the condition of anonymity. These interviews were particularly important in order to better understand the actual functioning of intelligence cooperation including the challenges and practicalities of overseeing different forms of cooperation versus how international intelligence cooperation is portrayed in laws and in theories. Lastly, as mentioned in the preface, the guide benefitted from the guidance and feedback of the project advisory board consisting of current and former overseers, intelligence officials, and experts.

Endnotes

1. US, White House, Press Release, "FACT SHEET: U.S. Efforts to Assist the Nigerian Government in its Fight against Boko Haram," 14 October 2014.
2. United Nations Security Council (UNSC) Resolution 2178, "Threats to international peace and security caused by terrorist acts," 24 September 2014.
3. "War On Terror, Kenya's Intelligence Partnership With CIA, Ethiopia, & NISA To Combat Al-Qaeda & Its Affiliates In East Africa," *Strategic International News*, 24 March 2015.
4. Philipp Hayez, "National oversight of international intelligence cooperation," in *International intelligence cooperation and accountability*, ed., Hans Born, Ian Leigh and Aidan Wills, (London: Routledge, 2011), 151-169.
5. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (Arar Commission), *Report of the Events Relating to Maher Arar: Analysis and Recommendations*, (Ottawa: Canadian Government Publishing, 2006), 431.
6. Helga Hernes, "Foreword," in *International intelligence cooperation and accountability*, xi.
7. For a review of the literature, see *International Intelligence Cooperation and Accountability*, in particular Chapter 1 "Accountability and intelligence cooperation" drafted by Ian Leigh, 4-6.
8. For further reference, see Andrea Wright, "Fit for purpose? Accountability challenges and paradoxes of domestic inquiries" and Hans Born and Aidan Wills, "International responses to the accountability gap: European inquiries into illegal transfers and secret detentions" in *International Intelligence Cooperation and Accountability*.
9. European Parliament, Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee), *Inquiry on electronic mass surveillance of EU citizens: protecting fundamental rights in a digital age*, 2013-14.
10. Council of Europe, Committee on Legal Affairs and Human Rights of the Parliamentary Assembly (Rapporteur Pieter Omtzigt), *Mass Surveillance*, 2015.
11. Council of Europe, European Commission for Democracy through Law (Venice Commission), *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies*, 2015.
12. Commissioner for Human Rights of the Council of Europe, *Democratic and effective oversight of national security services*, Issue paper (Strasbourg: May 2015).
13. These two expert studies are: Mathias Vermeulen, *The Snowden revelations, mass surveillance and political espionage*, 23 October 2013 and Annemie Schaus, *Advice on the Belgian regulations for the protection of privacy regarding methods of mass surveillance on data related to individuals, organisations, companies or institutions in Belgium or with links to Belgium*, 27 November 2013.
14. Intelligence and Security Committee of Parliament, *Privacy and Security: A modern and transparent legal framework*, (London: House of Common, 2015).
15. It concerns ongoing investigation (as of August 2015), See (in Dutch): *Investigations into the compliance of the General Intelligence and Security Service and the Military Intelligence and Security Service with two Parliamentary resolutions.* [AIVD en MIVD onderzoek "uitvoering twee Kamermoties], The Review Committee for the Intelligence and Security Services (CTIVD).
16. Information about the mandate and functioning of the ad-hoc inquiry of the Bundestag into the "NSA Affair" [NSA *Untersuchungsausschuss*] can be found here, https://www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss.
17. In some states services are mandated to disrupt or to prevent threats to national security.
18. Hans Born and Gabriel Geisler Mesevage, "Introducing intelligence oversight," in *Overseeing Intelligence Services – A Toolkit*, ed., Hans Born and Aidan Wills, (Geneva: DCAF, 2012), 6-17.
19. Aidan Wills and Hans Born, "International intelligence cooperation: Formidable challenges and imperfect solutions," in *International intelligence cooperation and accountability*, 278-279.
20. Arar Commission, *Report of the Events Relating to Maher Arar*, 472-482.
21. More information about EOS Committee can be found here, http://eos-utvalget.no/english_1/
22. Hans Born, Ian Leigh and Aidan Wills, ed., *International Intelligence Cooperation and Accountability*, (London: Routledge, 2011).

Part I: International Intelligence Cooperation

2

Nature and Scope of International Intelligence Cooperation

2.1 Introduction

International intelligence cooperation is the liaison or collaboration between state bodies, from one or more countries, responsible for the collection, analysis and/or dissemination of intelligence for purposes including defence, national security and the prevention and detection of serious organised crime. Such bodies encompass autonomous civilian or military intelligence and security agencies with domestic and/or foreign mandates (e.g. France's DGSE and the Canadian Security Intelligence Service – CSIS); departments within executive ministries (e.g. in foreign and interior ministries); units within armed forces; and so-called "joint analysis" or "fusion centres" (e.g. Belgium's Coordination Unit for Threat Analysis – CUTA). Some domestic intelligence services have law enforcement powers and are essentially security police (e.g. Norway's Police Security Service – PST). Others function purely to gather and assess intelligence on threats. Included among these institutions are bodies whose functions include the collection of human intelligence (e.g. the UK Secret Intelligence Service) or electronic and signals intelligence (e.g. the US National Security Agency – NSA). For the purposes of this guide, the term "intelligence service" (or "service") will be used broadly to refer to any of the aforementioned entities. The term of art used to describe relations with foreign services is "intelligence liaison." However, this guide uses the broader term "intelligence cooperation" because it better captures the fact that services do more than simply liaise and exchange information with

their foreign counterparts. As discussed in this chapter, services increasingly engage in covert operational cooperation, particularly in the area of bulk electronic surveillance.

Intelligence services also cooperate with foreign law enforcement agencies (e.g. police and border services), particularly through the sharing of information (see Box 2.1 for an example). Although this guide focuses on intelligence services, the regulation and oversight of such relationships fall within its scope. This guide will not, however, address international cooperation that falls exclusively within the law enforcement field or takes place primarily for law enforcement purposes, for example, in the legal preparation of cases for prosecution or deportation. The principal difference between international cooperation in the intelligence and security field and in the law enforcement realms is that, unlike most law enforcement bodies, intelligence and security services do not cooperate for the primary purpose of bringing criminal proceedings.[1] Most intelligence and security services' primary functions are collecting and analysing information to inform decisions by policymakers, military commanders, police investigators and border/customs agencies about threats to national security and other core national interests. This focus is reflected in their cooperation with foreign counterparts.

This chapter provides an overview of international intelligence cooperation by outlining the main forms of cooperation, the range of bodies that are involved, why services cooperate with foreign partners and the main subjects on which they cooperate. We will also use this chapter to reflect on some of the historical and current trends in intelligence cooperation. Before venturing into the details of international intelligence cooperation, we shall consider different ways of in which such collaboration much be conceptualised.

2.2 Conceptualising international intelligence cooperation

At the heart of most international intelligence cooperation is an exchange of "goods" or "services" – a quid pro quo. International intelligence cooperation is sometimes viewed as a marketplace, albeit with many transactions based on long-term strategic interests, not on item-for-item or item-for-payment trading. While information is the currency that is most often exchanged, services (and their governments) may also provide foreign partners with technical support, training, financial resources, diplomatic backing and space to host facilities (see below for further discussion). The *quid pro quo* is not necessarily an exchange of like-for-like items. For example, a service that is a large global player may provide a partner service in a smaller state with equipment and training and, in return, the recipient service might provide information or even conduct surveillance on the other service's behalf.[2] Alternatively, a state whose service has comparatively poor information collection capacities might provide valuable diplomatic support to another state in exchange for information.

Services normally "trade" on this market place when it serves their own nations' interests and there is generally a convergence of national interests underpinning bilateral or multilateral cooperation. On occasions, however, specific national requirements may lead services to trade with foreign counterparts that do not share their political outlook and may even be potential adversaries (for example, on the basis that my enemy's enemy is

my friend). The Iran Contra affair and Israeli intelligence services' liaison with Hamas over prisoner exchanges are but two examples.

International intelligence cooperation can be viewed as another mode of intelligence collection. As services use human sources and electronic surveillance to collect intelligence, they also liaise with foreign partners to gather intelligence. Services invest resources in their sources and methods, and they look to the international intelligence marketplace to secure information from foreign partners. Hence, some cooperation has been described as a form of "subcontracted intelligence collection based on barter."[3] The relative significance of information provided by foreign partners as a method of collection depends *inter alia* on a service's own collection capabilities and the subject matter. Small and medium-sized states generally rely extensively on larger partners for their information. Yet even states with major intelligence capabilities have gaps in their coverage and can benefit from receiving information from foreign services. It has been estimated that as much as 60% of the Cold War-era CIA intelligence product came from cooperating foreign services.[4]

Intelligence cooperation can also be viewed as an extension of foreign relations. In many states intelligence services are very close to the executive and their work is closely aligned with the priorities of the incumbent government. Generally speaking, intelligence cooperation will follow a state's foreign relations – a close diplomatic relationship is likely to be reflected at the level of intelligence services. This is also true of multilateral politico-military alliances such as NATO.

Intelligence cooperation also serves an instrument of foreign relations and even the development of policy. Former senior South African intelligence official, Barry Gilder has described intelligence cooperation as both a "tool of influence" in interstate relations and "a channel of ideology and attitude."[5] Tasking intelligence services with supporting the development of a new (helpful) service in an emerging democracy is one example. Threats and promises of increased or decreased intelligence cooperation may be used as leverage in foreign relations. For example, for a period, the US cut off intelligence cooperation with New Zealand to punish Wellington for its ban on ships carrying nuclear weapons entering NZ harbours.[6]

In some cases, intelligence relations with particular states and groups, such as terrorist organisations, are not aligned with publicly declared foreign relations. Governments may use intelligence relationships to pursue goals that are not publicly acknowledged. The secretive nature of international intelligence cooperation provides an opportunity for relations with services from states with which a service's government may not have close or any diplomatic relationships. The pre-1994 relationship between Israel and Jordan is a good example.[7]

A disconnection may arise between foreign policy and intelligence relations should intelligence professionals and their foreign partners take a different view of situations to their respective governments, or when they simply resist the impact of foreign policy changes on long-standing intelligence friendships. One example is the CIA allegedly

providing training and equipment to foreign services, such as to the Israeli intelligence services in the 1950s, in violation of official government policy on the provision of aid to a particular country.[8]

Principles of democratic governance require that services' foreign liaisons are subordinated to the policies of the incumbent government and consistent with the state's foreign policy. This is one reason for which executive control and oversight of international intelligence cooperation is important (see Chapter 6).

2.3 Taxonomy of international intelligence cooperation

This section will outline five types of international intelligence cooperation:

1. information sharing;
2. covert operational cooperation;
3. hosting facilities and equipment;
4. training and capacity building; and
5. providing hardware and software.

Most intelligence services do not engage in all of these forms of cooperation. For many services, cooperation with foreign partners is limited to information sharing; this form of cooperation will be the focus of this guide.

INFORMATION SHARING

Types of Information

Information sharing is the primary form of intelligence cooperation. The information exchanged can be divided into three levels. The first is ***strategic information***, which normally consists of assessments of foreign policy developments, security environments, and broad trends relating to threats such as WMD proliferation or extreme right movements. Such assessments are primarily written for policy makers by intelligence analysts in services or central analytical bodies like the UK's Joint Intelligence Committee. They include so-called "national intelligence estimates." Strategic assessments are most likely to be shared with bodies responsible for similar analyses in foreign governments or at international organisations such as NATO and the EU (whose Intelligence Analysis Centre [INTCEN] also generates its own assessments that are shared with member states). Although classified, these assessments would not normally reveal information about intelligence sources and methods, are generally viewed as being less sensitive than other forms of intelligence, and can potentially be shared more broadly.

Operational information typically pertains to the capabilities and modus operandi of specific armed forces, non-state groups and individuals considered to be a threat to security. Operational information also includes threat assessments relating to, for example, third countries, the security of diplomatic missions, and travellers in the country concerned. Such information is normally regarded as being of relevance in the first

instance to security experts rather than policymakers. Joint analysis or fusion centres such as Belgium's Coordination Unit for Threat Analysis (CUTA) and the UK's Joint Terrorism Analysis Centre (JTAC) are often the producers and exchangers of this type of intelligence, often based on an assessment of multiple inputs. Operational information can also include lines of intelligence reporting bearing on the strategic assessment of policy issues, such as the German BND reports on the debriefing of Curveball (see Box 3.1, Chapter 3), which influenced strategic assessments of Iraq's assumed pre-war WMD programmes; such reporting does not normally make references to the sources.

The third level of information is ***tactical information*** relevant to current operational investigations or military operations including, in the case of terrorism, for instance, specific details on the identity, location and activities of wanted individuals, arms caches, and targets. This information is relevant to answering questions about who, what, where, when, and how. It often relates to or is derived from ongoing intelligence or security operations. Military intelligence services share large amounts of tactical information in theatres of armed conflict, such as the NATO-led operation in Afghanistan, often in "real time." In a "civilian" context, tactical information may, for example, be provided on the movements of a suspected terrorist or serious organised criminal, or the procurement intentions of a WMD proliferator. Tactical intelligence is normally regarded as the most sensitive category of information because it being revealed could compromise the success of operations and techniques, and the safety of the people involved. Accordingly, this type of information is shared strictly on a need-to-know basis and normally on a bilateral level between professionals where a pattern of trust has already been established over time.

Whether or not information shared between services is "raw" intelligence, an analysed "end product" or an all source assessment depends largely on the need for specificity and timeliness. How the intelligence was collected may also affect the nature of the information exchanged. Some services exchange raw signals, electronic intelligence, and military imagery with equivalent services in other countries. This has, however, been described as a "far reaching" form of cooperation by a Dutch oversight body and is only likely to occur if they have a close, trust-based relationship.[9] For example, the United Kingdom – United States of America Agreement (UKUSA or "Five Eyes") alliance partners exchange raw data obtained from intercepting cable bound or satellite communications (see Box 2.3). Human intelligence is, however, very rarely exchanged in its rawest forms because services are extremely sensitive about providing information that could reveal the identity of their sources. Even for closely cooperating services the source is likely to be well disguised in the reporting with only descriptors such as regular and reliable, new source on trial, or documentary being used to guide the user.

Reactive Versus Automated Information Sharing

Intelligence is most commonly shared in response to requests from a foreign partner for any information bearing on a specific topic, group, or individual. This is normally the case with regards to tactical information shared between services; a service may, for example, request information about the movements of a suspected terrorist cell.

A service receiving a request from a foreign partner may already possess pertinent information to share, but in the case of terrorism or serious crime, it may also have to undertake surveillance operations to gather the requested information. By way of example, it has been reported that NATO states with bases in Germany had a long-standing agreement whereby they could request the German services to conduct surveillance operations for the purposes of obtaining information to protect their forces.[10] Undertaking intelligence collection operations at the behest of a foreign service gives rise to important legal and accountability questions that will be addressed in Chapters 3 to 5. When services conduct surveillance for a foreign partner, they should remain bound by their own legal framework, including the rules governing when and how surveillance measures can be used. British legislation governing intrusive investigation, for example, makes specific provision for meeting requests under the provisions of mutual assistance agreements.[11]

Information sharing may also be proactive or even "automatic," meaning that it occurs in the absence of a specific request. This is more likely to occur when two or more states have very close cooperation on particular issues or threats and they know what their partners are interested in. Where patterns of cooperation exist, each service will be aware of the potential interests and capabilities of the other, and, therefore, information may be volunteered without a request having been made. This may occur if the information may bear on the ability of the partner nation to manage, for example, a threat to tourists or commercial interests in the country concerned. Automatic exchanges are also common in regard to strategic assessments (see above). Whether or not information is received upon a request made to a foreign service or provided without it having been requested can have significant implications regarding the legal position of the recipient service. This is particularly true with regards to incoming information that may have been obtained in violation of human rights. These questions are addressed in detail in Chapters 4 and 5.

HOW INFORMATION IS SHARED

Intelligence services use many different methods for sharing information with foreign services; this subsection will outline several of these. The methods used for sharing information have implications for oversight and accountability because they may result in different (or no) written records ("paper trails"). The ability of oversight bodies to evaluate intelligence services' international intelligence cooperation activities, including information sharing, is shaped by how well such activities are documented (see Chapter 7).

Many bilateral intelligence relationships continue to centre on the traditional liaison officer system whereby information is shared through liaison officers posted in the services' respective capitals. Services with very close relationships may even host respective liaison officers in their headquarters. Liaison officers remain the pre-eminent vehicle for information sharing primarily because exchanges are based on trust and services prefer to share information through persons with whom they have developed personal relationships.[12] Information is usually shared through meetings; the persons involved subsequently draft reports that are then transmitted to headquarters. Generally, information is shared in the capital of the country for which the information has most

relevance. If, for example, country A's intelligence service has information about a terrorist group in country B, the information is most likely to be shared through country A's liaison officer in the capital of country B. Services also use liaison officers to share information with international bodies, such as the ICTY, and within multilateral intelligence platforms, like the EU INTCEN.

Some intelligence services have secure electronic links with close partners, and these are also used for direct information sharing. An increasing amount of information is exchanged electronically through direct headquarters-to-headquarters transfers. On a multilateral level, there is, for example, a secure electronic system connecting services in the Club of Berne (CdB).[13] Similarly, the sharing of defence intelligence between NATO allies typically occurs through common membership of secure intelligence networks.

Information of a strategic nature may also be exchanged in the context of intelligence service delegations visiting their foreign counterparts. These visits typically involve very senior officials and agency leads on specific issues. By way of illustration, it was recently revealed that senior delegations from Germany's principal intelligence services have frequently visited the NSA to discuss cooperation.[14] Visits of this nature would not normally involve the exchange of detailed operational or tactical information but are used for more strategic discussions or to lay the groundwork for subsequent direct information sharing. Some ministers responsible for intelligence and security may also exchange strategic information during meetings with their foreign counterparts. This is more likely if ministers have a strong personal interest in intelligence, as well as in countries that have dedicated intelligence ministers, such as South Africa.

In some close intelligence cooperation relationships, information is increasingly "shared" by one or more services directly accessing certain categories of information, which may have been gathered by a foreign partner, held by a partner or in joint databases. In other words, information is not literally shared because a partner can access it directly. The main example (in the public domain) of this type of arrangement is the relationship between the NSA and Government Communications Headquarters (GCHQ); the UK government has acknowledged that GCHQ was permitted to access directly banks of raw data gathered by the NSA and other agencies.[15] Direct access occurs not only amongst Five Eyes partners (see Box 2.3); according to testimony from a former director of DGSE (France's foreign intelligence service) Western services have direct access to joint databases.[16]

COVERT OPERATIONAL COOPERATION

Covert operational cooperation between intelligence services goes beyond the exchange of information. It involves services collaborating on secret activities in pursuit of a common objective or their own independent aims within a shared strategic outlook. This category of international intelligence cooperation can range from joint surveillance operations to complex disruption and sting operations or backchannel diplomacy based on secret intelligence, such as the US/UK operation in 2002/3 to force Colonel Gaddafi to give up his weapons of mass destruction. Such collaboration may take place on the territory of one of the services involved or in third states. This subsection focuses on providing an overview

of the types of covert operational cooperation that may take place. The domestic and international legal frameworks governing covert operational cooperation, as well as the legality of particular forms of operational cooperation are addressed in detail in Chapters 4 and 5.

Covert operational cooperation often involves intelligence officers working alongside foreign counterparts on the same operation. Officers from several services may physically work together on, for example, a surveillance operation. This may occur in a third state, such as the joint surveillance work conducted by NATO allies in Afghanistan. However, services also run joint surveillance operations on their own territory. The "home" service might provide the manpower and access for an operation while their foreign partner provides the equipment and expertise through their station in the country. The *Treholt* case in Norway is an example of joint surveillance operation whereby the Norwegian Police Security Service (PST) worked closely with a foreign partner to surveil a suspected Soviet spy in Oslo. The foreign service played a role in planning the operation and provided some surveillance equipment and expertise, including installing devices.[17] Another example of a joint operation that has come to light is the UK Security Service-led Operation Samnite in 2001 (see Box 2.1).

Box 2.1: Operation Samnite

Operation Samnite was a 2000-1 UK Security Service-led sting operation against the Real IRA (Irish Republican Army), which included cooperation from a number of foreign services. UK intelligence officers posed as Iraqi intelligence agents willing to sell weapons (including rocket-propelled grenades) to the Real IRA. They held a number of meetings with the would-be buyers in Hungary, Austria and Slovakia. The suspected terrorists were kept under surveillance with the support of local services and ultimately arrested in a joint operation between Slovakian armed police and the UK Security Service.[18]

Joint surveillance operations of this nature are less common than services simply asking their foreign counterparts to place an individual/group under surveillance. However, foreign intelligence officials might be directly involved if, for example, a foreign service has particular expertise in certain types of surveillance or if an influential foreign partner wished to ensure that it maintained some control over surveillance operations conducted in a partner service's territory.

Beyond cooperation in the context of individual surveillance operations, various intelligence services may cooperate in the collection and analysis of SIGINT on an ongoing basis. Recently-disclosed documents indicate that a significant number of countries have cooperated in a large-scale NSA programme for the interception of electronic communications passing through international fibre optic cables and other networks. This apparently involves NSA partners tapping fibre optic cables on their state's territory (including with equipment provided by the NSA, which services may also use for their own collection activities) and the data collected is transmitted to the NSA.[19]

Some intelligence services jointly run surveillance and analysis facilities and/or station staff with foreign partners for the purposes of carrying out joint intelligence collection

and analysis on an ongoing basis. The Five Eyes partnership (see Box 2.3, below) is one example of this. NSA staff work alongside foreign counterparts on an ongoing basis at, *inter alia*, SIGINT facilities at Pine Gap in Australia and Bude in the UK.[20] Capturing the extent of ongoing SIGINT cooperation between the US and UK, a former director of the UK Security Service has stated that the recipients/customers of some SIGINT seldom know which country generated the access the data or the intelligence "product."[21] A further example of long-term operational cooperation in the collection of SIGINT is the recently revealed collaboration between the NSA and Germany's BND (see Box 2.2).

Box 2.2: US-German signals intelligence cooperation at bad aibling[22]

The Snowden revelations and a subsequent Bundestag inquiry have shown that the NSA and BND engaged cooperation in the collection and analysis of SIGINT at Bad Aibling, a satellite interception station in Bavaria. Previously operated by the NSA, Bad Aibling was handed over to the BND in 2004 with the understanding that information gathered would be shared with the NSA. An NSA team remained on site at Bad Aibling and retained its own installation. Joint working groups were established for the acquisition of data (Joint SIGINT Activity) and for the analysis of collected data (Joint Analysis Centre) – these involved agents from both services working side-by-side.

Cooperation centred on the BND gathering data on behalf of the NSA on the basis of lists of thousands selectors (provided by the NSA) relating to, for example, telephone numbers and internet identifiers (e.g. email addresses). The BND electronically filtered the requested selectors for legal compliance and the protection of German interests, before entering (apparently) permissible NSA selectors (along with the BND's own selectors) into collection systems to gather data. Following further filtering, the data gathered was forwarded to the NSA. It has been reported that, in return, the NSA provided sophisticated surveillance and analysis technology. Following accusations that this cooperation involved the BND conducting unlawful and/or politically unacceptable surveillance, activities at Bad Aibling (and elsewhere) were subjected to an ongoing Bundestag inquiry.

Some intelligence services have cooperated with foreign counterparts in the covert and illegal apprehension, transfer, *incommunicado* detention and interrogation of persons deemed to pose a threat to security. In the context of combating Jihadist terrorism, a number of services have played a part in a US intelligence-run system of extraordinary rendition and arbitrary detention. Services' covert operational involvement has ranged from abducting suspected terrorists and transferring them to detention facilities, to allowing such facilities on their territory, to being present at interrogations. For example, Italian and Macedonian services worked with US intelligence to abduct, detain and render Abu Omar and Khaled El Masri from Italy and Macedonia respectively (see Chapter 3). The CIA has also transferred suspected terrorists for detention and questioning by foreign intelligence services. Information gleaned from these processes was then shared with the US. These practices have given rise to serious concerns over human rights violations and a litany of inquiries, civil and criminal proceedings (see Chapters 3-4 and 8).

HOSTING FACILITIES AND EQUIPMENT

States may host facilities or infrastructure that are used or operated exclusively by a foreign intelligence service or armed forces. An infamous example of hosting facilities is the so-called black sites run by the CIA in various European and Asian countries and used for the purposes of detaining and interrogating suspected terrorists captured in other parts of the world. Hosting facilities does not necessarily amount to covert operational cooperation because the host state is not necessarily aware of or involved in the operations conducted therein/there from.

There is also a long history of states hosting SIGINT facilities run by or in collaboration with foreign intelligence services. For example, Germany, UK and Denmark, among others, have permitted the US to construct or use signals intelligence interception facilities on their respective territories.[23] Such hospitality may be part of the arrangements for mutual assistance, such as the NATO Treaty, take place under a bilateral status of forces agreement, or on a more informal and ad hoc basis. Host states may authorise another state and its intelligence services to operate facilities in exchange for resources, diplomatic support, or rights to make use of surveillance infrastructure or information gathered by surveillance facilities.

Short of hosting facilities, states also host equipment of foreign intelligence services and/or grant them access to infrastructure, such as communications cables (see above for an example from the Snowden revelations).

TRAINING AND ADVICE

Providing advice and training to foreign intelligence services (and in some cases their governments and parliaments) is another form of international intelligence cooperation. Western intelligence services have played proactive roles in security sector reform processes in numerous transition states. The provision of advice and other resources has extended to assisting in the creation of entire agencies. The US services played an instrumental role in the creation of South Korea's principal intelligence agency and Germany's BND after the Second World War.[24] A further example is the Federal Bureau of Investigation's (FBI) apparent involvement in training Israeli Shin Bet (domestic intelligence) officers in the 1950s and 1960s.[25] More recently, assistance from Western services was central to the development of services of central and Eastern Europe in the 1990s and beyond.[26]

There is also a long tradition of established services providing training and equipment to services in developing countries. For instance, intelligence services from both blocs trained and advised the services of African countries aligned to their respective blocs.[27] Training also occurs between well-established intelligence services. Recent revelations about the German services' educational trip to the NSA are a case in point. The NSA is alleged to have provided German services with advanced surveillance software and officers trained in its use.[28] The provision of training to other states' intelligence services has focussed and continues to focus on enhancing their operational effectiveness, but it may also centre on seeking influence a foreign counterpart's threat perceptions and

priorities. Services also provide such training to ensure that their foreign counterparts become more effective international intelligence cooperation partners.

Beyond operational training and advice, some services have contributed to the development of legislation and the design of intelligence oversight mechanisms in new democracies, as was the case in Bosnia and Herzegovina and Kosovo. Moreover, Western intelligence services frequently provide human rights training to reformed or newly created services.[29] Promoting human rights compliance by foreign services should be in the interests of democratic states' intelligence services, because it can foster the development of partners that are legally and politically "safer" to work with. This is particularly true in light of the high-profile problems that have emerged from working with intelligence services that do not respect human rights and are not accountable (see Chapter 3).

It is axiomatic that the provision of training and advice is not an altruistic offering; there is, of course, a "*pro quo*" where there is a "*quid.*" Services do this with the aim of fostering the development of 'friendly' foreign services that share their perspectives and priorities. This may extend to exerting significant influence on a foreign service's threat assessments and, in turn, a government's security policies (see Chapter 3). They undoubtedly expect to see the foreign service responding to their priorities and providing information in return for the support provided.

PROVIDING HARDWARE AND SOFTWARE

Training is often accompanied by the provision or lending of hardware and software to foreign services. What is provided depends on the recipient's level of 'development' and the closeness of the services. Examples range from the provision of basic surveillance equipment to fledgling services in a transition state to the NSA's provision of sophisticated signals intelligence software such as XKeyScore to other Five Eyes partners.[30] Recent revelations suggest that, in some cases, surveillance equipment is provided with the expectation that data gathered through the use of that equipment will be shared with the service providing it.[31]

2.4 Institutions involved in international intelligence cooperation

The nature of the actors involved on the various sides of an international intelligence relationship depends on the composition and division of labour within the intelligence communities of the countries involved. An intelligence and security service may have several interlocutors in another state; it may, for instance, have a relationship with the other state's domestic security service, a foreign intelligence service, or a joint analysis centre. However, cooperation is not necessarily between the same types of entities on all sides of a relationship. This may be for historical reasons or the result of the fact the states involved do not have analogous services. For example, some states have subsumed domestic intelligence functions under the police, and many states do not have (or admit to having) foreign/external intelligence services. Nevertheless, services with similar

specialisations (e.g. counterintelligence or signals intelligence) tend to work more closely with their equivalents in other states.

Many services have bilateral relations with hundreds of foreign services, and they may have several counterparts in some countries. For example, in 2013 the director general of the DGSE stated that his service works with more than 200 foreign partners.[32] The depth and regularity of contact will vary. Relations may range from the existence of a cooperation agreement that is rarely used, to occasional meetings and exchanges of information, to regular information sharing on select issues or certain types of intelligence, to extensive daily cooperation of different forms and spanning a range of issues.

While the majority of international intelligence cooperation remains bilateral, there have long been prominent multilateral intelligence cooperation platforms set up to support multilateral responses to challenges. Since its creation, NATO has had multilateral intelligence staff as part of the International Military Staff at NATO HQ, and NATO Commands likewise have so-called J2 intelligence organisations staffed by NATO members. Multilateral military operations, such as the NATO action in Kosovo and Afghanistan, are accompanied by extensive in-theatre, tactical intelligence sharing. Beyond military action, multilateral initiatives vary from the institutionalised cooperation within bodies such as the EU's Intelligence Analysis Centre, whose role is limited to producing assessments, and the Committee of Intelligence and Security Services of Africa (CISSA), to looser "clubs" that are not based on any formal agreements and in which information is periodically exchanged. One such example is the CdB that consists of periodic meetings of senior European intelligence officials to discuss matters of common interest. It includes a Counterterrorism Group that at aims at improving operational cooperation between services, the provision of joint training and exchange of some strategic and operational information.[33]

The aforementioned examples of multilateral cooperation include 29 services in the case of the CdB and 50 at CISSA. Multilateral cooperation also takes place among small groups of services with the oldest example being the UKUSA alliance (or Five Eyes network), which since the Second World War has centred on signals intelligence (SIGINT) cooperation (see Box 2.3). An example of multilateral international intelligence cooperation that went beyond information sharing and joint analysis was Operation Condor in 1970s South America (see Box 2.4). Cooperation is generally more extensive and involves sharing of more sensitive information when there are smaller number of states involved – the premise being that the more people who have access to sensitive information, the less secure the information is.

Box 2.3: UKUSA Agreement (Five Eyes)

UKUSA is an intelligence cooperation relationship between the signals intelligence agencies of the US, UK, Canada, Australia and New Zealand. With its origins in Anglo-American SIGINT cooperation in World War Two and reinforced by the need to support the UN action during the Korean War, the alliance developed to help understand the military threat posed by the USSR. UKUSA is based on a series of agreements and memoranda of understanding dating back to the 1940s and 1950s.

Cooperation centres on the covert interception and decryption of all types of wanted communications, not just those of military forces, as well as the analysis and exchange of intelligence derived from interception. With the development of modern telecommunications networks and the internet, the cooperative effort to locate and monitor the communications of targets of interest, including terrorists, serious criminals, proliferators and states is now carried out by the interception of global communications channels. Interceptions may target specific communications but are commonly untargeted meaning that swathes of traffic are intercepted and then analysed for persons or subjects of interest. The so-called Echelon system is said to integrate the various components of the collection network (with more than five billion interceptions per day), drawing together collected information into a system (databases) that can be accessed by all partners for predefined purposes.

Geographical coverage is one of UKUSA's key strengths; all of the partners have interception facilities and some host NSA satellite ground station facilities such as Pine Gap in Australia and Menwith Hill in the UK. Bound by shared security of information protocols, the partners also increasingly work together to improve cybersecurity. Cooperating services exchange and second personnel to promote greater integration.

UKUSA partners share many strategic priorities on which their efforts are collective, but services also use their national facilities to pursue their own targets and priorities, although they may request partners' assistance in doing so.[34]

TRENDS AND TRAJECTORIES IN INTERNATIONAL INTELLIGENCE COOPERATION

While international intelligence cooperation has come to public prominence over the past decade, it is not a new phenomenon. Information sharing has long been an integral part of interstate relations and states' intelligence services have been working together for at least a century. Rudimentary information exchange (particularly tactical information on German troop movements) initially came to the fore during the First World War, which also saw cooperation on signals intelligence between, for example, the British Army and American Army signals organisations after the US had entered the war in 1916.[35] The Second World War (WW2) saw further and more extensive cooperation including between US and British Commonwealth signals intelligence organisations. Although modern international intelligence cooperation has its roots in wartime, peacetime intelligence cooperation developed significantly after WW2 on both sides of the Iron Curtain. Perhaps the best

known international intelligence relationship – the Five Eyes cooperation arrangement between the US, UK, Canada, Australia and New Zealand – dates back to 1947 (see Box 2.3).

The scope and volume of international intelligence cooperation is greater now than ever before. Writing nearly twenty years ago, Michael Herman, a former senior British intelligence official, suggested that most Western intelligence output is exchanged with someone (overseas).[36] More recently, a senior UK counter-terrorism official stated in the context of recent legal proceedings stated that:

> intelligence that foreign governments share with the (UK) intelligence services […] represents a significant proportion of the intelligence services' total store of intelligence on serious and organised criminals, terrorists and others who may seek to harm UK national security.[37]

Given that this statement was made in relation to a state that has a relatively large and well-resourced intelligence community, it is likely that significance of intelligence shared by foreign services is even greater for states that have smaller and less well funded intelligence communities.

As the requirements placed on intelligence services have evolved, so too have the focuses of their international cooperation. Accordingly, the main shift has been from cooperation to meet threats posed by states to cooperation relating to threats posed by non-state actors. This shift had already begun after the Cold War but was expedited by the attacks of 11 September 2001. Indeed, Western services received criticism for not having cooperated enough with foreign partners prior to 9/11 and they came under major pressure to increase cooperation.[38] The United Nations Security Council in Resolution 1373 expressly encouraged intelligence sharing on terrorism. Cold War-era intelligence cooperation had largely focused on static threats, such as conventional and nuclear force capabilities, and counterintelligence, whereas contemporary intelligence cooperation primarily addresses more mobile threats posed by individuals and groups.

Intelligence cooperation relationships and networks have evolved in response to perceived threats to the national security of the states involved. Military operations, such as those in the former Yugoslavia and more recently in Libya have reinforced the need for intelligence cooperation. The expansion of international terrorism and organised crime networks with members and resources in many states has also required services to work with their international counterparts on a growing range of issues. Because the majority of states now face threats that have trans-border components, a growing number of intelligence services are cooperating with foreign services. The evolving nature of threats – particularly terrorism – has caused Western services to develop relationships with foreign services with which they had limited history of cooperation. Cooperation with these so-called 'non-traditional partners' (from a Western perspective) has given rise most of the concerns about the lawfulness and ethicality of international intelligence cooperation (see Chapter 3).

SUBJECTS OF INTERNATIONAL INTELLIGENCE COOPERATION

Subjects of international intelligence cooperation vary between regions and over time. Much depends on how dominant global and regional players perceive and define threats. During the Cold War, the focus of intra-bloc intelligence cooperation was the threat posed by the other side. Since the late 1990s, terrorism is the threat that has given rise to the most high-profile international intelligence cooperation. Politically and legally, it has been recognised as an issue that demands international intelligence cooperation, particularly information sharing. To a lesser extent, the proliferation of weapons of mass destruction and organised criminal networks are subjects of international intelligence cooperation. It is likely that cyber hackers and cyber criminals will increasingly be a focus of cooperation between services.

Regardless of the demands of the US and EU or even the UN Security Council, jihadist terrorism is not viewed as a significant priority in all regions, and this is undoubtedly reflected in the focus of regional intelligence cooperation. In the Western Balkans, for example, policymakers and security establishments view organised crime as a far greater threat to national and regional security.[39] Another example of a specific regional, albeit nefarious, focus of international intelligence cooperation is the Operation Condor's pursuit of left-wing groups in 1970s South America (see Box 2.4).

Box 2.4: Operation Condor

Operation Condor was an extensive multilateral intelligence cooperation initiative between six South American states in the 1970s (Chile, Argentina, Uruguay, Paraguay and Bolivia were founding members; Brazil, Ecuador and Peru were more peripherally involved later). Initiated by Chile's military intelligence service, Operation Condor was aimed at defeating national and continent-wide leftist movements, some of which were engaged in subversive activities. Operation Condor included three forms of intelligence cooperation: (a) operational and tactical information sharing, including the creation of a central data bank; (b) joint surveillance, renditions and interrogations of (suspected) members of leftist groups; and (c) and joint assassinations, including in Europe. The services also agreed to permit their partners to operate freely on their respective territories. Operation Condor was responsible for systemic human rights abuses including extrajudicial killing, forced disappearances and torture across the continent and beyond – it resulted in tens of thousands of deaths and disappearances.[40]

International intelligence cooperation is not only about threats to security. Services also share information about their experiences, perspectives on or interpretations of pertinent issues, technological developments, and even their oversight arrangements. For instance, the British services' counterterrorism experience in Northern Ireland was shared with close partners seeking to counter terrorist threats over the past decade.[41] Services also exchange views on methodologies for particular work, such as developing national intelligence estimates. International intelligence cooperation may also focus on promoting mutual understanding and identifying opportunities for conflict management and peace talks. African intelligence services' cooperation in the framework of CISSA is a

good example in this regard; the CISSA secretariat provides analyses to support African Union (AU) led conflict management efforts.[42]

Intelligence relationships are often 'multi-speed': the depth/extent of two or more services' relationships often varies according to the subject of cooperation. Two services may, for instance, cooperate very closely in the area of counterterrorism or counter-narcotics but have very limited exchanges (let alone joint operations) in the fields of counterintelligence or foreign policy. Services may be close collaborators in some areas, whilst being rivals in others, such as in collecting economic intelligence[43] or have areas of foreign policy that are off-limits for information exchange.

Endnotes

1. There is a growing convergence between the types of issues around which intelligence services cooperate with foreign partners and those addressed by police services. Activities such as (preparing) terrorism and the proliferation of WMDs are not only security threats, they are also criminal offences. Consequently, many of the individuals/groups that are the subjects of international intelligence cooperation may also be the subjects of international cooperation between law enforcement agencies.
2. By way of example, see the operation described by Henry Crumpton, *The Art of Intelligence: Lessons from a Life in the CIA's Clandestine Service*, (New York: Penguin, 2012), 90-92.
3. Jennifer Sims, "Foreign Intelligence Liaison: Devils, Deals, and Details," *International Journal of Intelligence and Counterintelligence* 19, (2006): 195-196.
4. Rhodri Jeffreys-Jones, *In Spies We Trust: The Story of Western Intelligence*, (Oxford: OUP, 2013), 188; Martin Rudner, "Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism," *International Journal of Intelligence and Counterintelligence* 17 (2004): 213.
5. Barry Gilder, *Songs and Secrets: South Africa from Liberation to Governance*, (London: Hurst, 2012), 212.
6. Richard Aldrich, *GCHQ*, (London: Harper Press, 2011), 444-447; Michael Herman, *Intelligence power in peace and war,* (Cambridge: Cambridge University Press, 1996), 213, 215-216.
7. This is discussed extensively in: Efraim Halevy, *Man in the Shadows*, (London: Phoenix, 2006), 70-118.
8. Ephraim Kahana, "Mossad-CIA Cooperation," *International Journal of Intelligence and Counterintelligence* 14, (2001): 413.
9. See for example: The Netherlands, Review Committee on the Intelligence and Security Services, *Review Report on the Processing of Telecommunications Data by GISS and DISS*, Review Report no. 38, (The Hague, 2014), 28.
10. Robert Reid, "Official: US, Germany to negotiate 'no spy' pact," *Associated Press*, 12 August 2013.
11. UK, *Regulation of Investigatory Powers Act 2000* c.23, s1(4); s5(1)(b)(c); s5(3).
12. Herman, *Intelligence power in peace and war*, 208.
13. Stephen Lander, "International Intelligence Cooperation: An Inside Perspective," *Review of International Affairs*, vol. 17 no. 3, (2007): 489.
14. Rene Pfister et al., "Secret Links between Germany and the NSA," *Der Spiegel*, 22 July 2009.
15. James Ball, "GCHQ views data without a warrant, government admits," *The Guardian*, 29 October 2014.
16. Testimony of Érard Corbin de Mangoux, Director General of DGSE, before the National Assembly's Defence Committee, (20 Feburary 2013).
17. Norway, EOS Committee, *The EOS Committee's investigation into the methods used by the Norwegian Police Surveillance Service (POT) in the Treholt case*, A Special Report to the Storting, (Oslo: 2011), 11-12.
18. Tom Parker, "Once More Unto the Breach: Britain's Forty Years on the Frontline of the War or Terror," in *Safety Liberty and Islamist Terrorism: European and American Approaches to Domestic Counterterrorism*, ed., Gary Schmitt, (Washington DC: American Enterprise Institute Press, 2010), 28; "Dissident republicans get 30 years," *BBC News*, 7 May 2002.
19. Anton Geist et al., "NSA 'third party' partners tap the Internet backbone in global surveillance program," *Dagbladet Information*, 19 June 2014; Ryan Gallagher, "How Secret Partners Expand NSA's Surveillance Dragnet," *The Intercept*, 19 June 2014; Council of Europe, Committee on Legal Affairs and Human Rights of the Parliamentary Assembly (Rapporteur Pieter Omtzigt), *Mass Surveillance*, 2015, para 42.
20. "Eyes Wide Open," *Privacy International*, 26 November 2013.
21. Lander, "International Intelligence Cooperation: An Inside Perspective," 487.
22. "Spying Together: German's Deep Cooperation with the NSA," *Der Spiegel*, 18 June 2014; "Spying Close to Home: German Intelligence Under Fire for NSA Cooperation," *Der Spiegel*, 24 April 2015; "America's Willing Helper: Intelligence Scandal Puts Merkel in Tight Place," *Der Spiegel*, 4 May 2015; Ian Traynor, "Cover-up claims over revelation that Germany spied on EU partners for US," *The Guardian*, 30 April 2015; "German BND didn't care much about foreign NSA selectors," *Electrospaces*, 12 May 2015.
23. Jeffreys-Jones, *In Spies We Trust*, 153, 170.
24. Herman, *Intelligence power in peace and war*, 202; Jeffreys-Jones, *In Spies We Trust*, 107-108.
25. Kahana, "Mossad-CIA Cooperation," 413.
26. Alex Martin, "The lessons of Eastern Europe for modern intelligence reform," *Conflict, Security & Development* 7, Issue 4, (2007): 552, 558-559; Larry Watts, "Intelligence Reforms in Europe's Emerging Democracies," *Studies in Intelligence*, 2004; Oldrich Cerny, "The aftermath of 1989 and the reform of intelligence: the Czechoslovakian

case" in *Democratic control of intelligence services: Containing Rogue Elephants*, ed., Hans Born and Marina Caparini, (Aldershot: Ashgate, 2007), 101.

27. Sandy Africa and Johnny Kwadjo, "Introduction," in *Changing Intelligence Dynamics in Africa*, ed., Sandy Africa and Johnny Kwadjo, (GFN-SSR, 2009), 8.
28. Rene Pfister et al., "Secret Links between Germany and the NSA."
29. Crumpton, *The Art of Intelligence*, 95.
30. See for example: Ryan Gallagher and Nicky Hager, "New Zealand Used NSA System to Target Officials, Anti-Corruption Campaigner," *The Intercept*, 14 May 2015.
31. Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe, *Mass Surveillance*, para 42.
32. Testimony of Érard Corbin de Mangoux, Director General of DGSE, before the National Assembly's Defence Committee, 20 February 2013.
33. Rudner, "Hunters and Gatherers," 210-211; Lander, "International Intelligence Cooperation: An Inside Perspective," 489; Klas Bergenstrand, (Director General of the Swedish National Security Service), address to the International Criminal Law Network, The Hague, 13 October 2004.
34. Aldrich, *GCHQ*, 7, 89-104, 345-346, 446-448; Martin Rudner, "Britain Betwixt and Between: UK SIGINT Alliance Stategy's Transatlantic and European Connections," *Intelligence and National Security* 19, No. 4 (2004); Lander, "International Intelligence Cooperation: An Inside Perspective," 487; Richard Norton-Taylor, "Not so secret: deal at the heart of UK-US intelligence," *The Guardian*, 25 June 2010; "Eyes Wide Open," *Privacy International*.
35. Herman, *Intelligence Power in Peace and War*, 200-201.
36. Ibid., 207.
37. Witness statement of Charles Farr in Privacy International, *Liberty and others v. Secretary State for Foreign and Commonwealth Affairs and others*, before the Investigatory Powers Tribunal, IPT/13/92/CH, 16 May 2014, para 20.
38. National Commission on Terrorist Attacks Upon the United States (911 Commission), *Final Report of the National Commission on Terrorist Attacks Upon the United States*, (Washington DC: 2004), 122.
39. Miroslav Hadžić, "Accountability of Statutory Security Actors in the Western Balkans," in *Almanac on Security Sector Oversight in the Western Balkans*, ed., Franziska Klopfer et al. (Belgrade: BCSP/DCAF, 2012), 226.
40. John Dinges, *The Condor Years*, (New York: The New Press, 2004), 18, 100-109, 116-125, 194, 222-226.
41. Eliza Manningham-Buller, "Lecture One: Terror," *BBC Reith Lectures 2011: Securing Freedom*, broadcast of BBC Radio Four, 6 September 2011.
42. Committee of Intelligence and Security Services of Africa (CISSA), *The Objectives of CISSA*, http://cissaau.org/about-cissa/objectives/.
43. Jeffreys-Jones, *In Spies We Trust*, 188.

3

Benefits and Risks of International Intelligence Cooperation

3.1 Introduction

This chapter will provide an overview of the benefits that intelligence services and their states can derive from cooperation with foreign intelligence services. It will then examine some of the risks associated with such cooperation. This discussion is particularly relevant for oversight bodies and members of the executive branch because it highlights a number of issues that they may wish to focus on in order to ensure that appropriate benefits are derived from international intelligence cooperation and that potential risks are managed as far as possible

3.2 Benefits of international intelligence cooperation

Intelligence services cooperate with foreign counterparts primarily because it benefits their own work and serves their country's national interest. International cooperation between intelligence services and between intelligence services and international organisations can also promote ends that are of universal benefit, such as the apprehension of war criminals or the prevention of the proliferation of WMDs. Perhaps most importantly, international intelligence cooperation can help to safeguard the right to life, and it can prevent serious threats to public safety. It is widely accepted that information sharing has contributed

to the prevention of numerous terrorist attacks over the past decade, saving many lives. In view of the current threat posed by transnational jihadist terrorist groups whose members can cross borders with relative ease, the importance of international intelligence cooperation may never have been greater. This section will provide an overview of the benefits of international intelligence cooperation across a number of areas.

MEETING THE NEED FOR INFORMATION AND RESPONDING TO EVOLVING THREATS

No state's intelligence services have the resources or expertise to counter all threats to their country's security (or international security) and public safety on their own. Services and their political masters have an insatiable appetite for information, but they will never have the capacity to satisfy this appetite through their own collection activities.[1] Cooperation with foreign services, primarily through information sharing, can enable a service to provide more complete and more timely intelligence to consumers of intelligence, including military commanders, law enforcement officials, and policymakers to improve the quality of decision making.

As was discussed in Chapter 2, the nature of threats faced by many states has shifted and diversified in the past two decades. International intelligence cooperation enables services to rapidly access information relating to issues, geographical areas, or communities that they may not have otherwise had access to. An example of this is the Indian-Canadian intelligence sharing in response to the threat of Sikh terrorist groups in the 1980s (see Box 3.2). Canada's services had limited knowledge of the individuals and groups whose aim was to strike Indian targets in North America as part of a separatist campaign being waged in India. Although, in this case, there was a failure to act on information provided by Indian intelligence services, threats of this nature illustrate why services have to cooperate with foreign partners to acquire relevant information. Acquiring information from foreign partners is especially critical in rapidly-evolving threat environments (including threats to tourists and businesses overseas) where services have significant gaps in their "coverage." A contemporary example of this is the rapid expansion of Boko Haram, a terrorist group, in West Africa. This group was initially a domestic concern for Nigeria, but its rapid advance across borders, posing a threat to neighbouring states such as Cameroon and Chad, has required greater regional intelligence cooperation.[2] Capturing the need for cooperation to meet gaps in coverage, former Director of the CIA, George Tenet, stated that after 9/11, US intelligence had to cooperate more closely with various services in the Middle East in order to avoid "walking through the Arab world wide open and half blind."[3]

The need to work with foreign counterparts has become more pressing with the globalisation of threats to security. Actors that threaten the security of one or more states can take advantage of the ever increasing ease with which persons, materials, information, and money can cross borders. Although these trends are especially evident with contemporary violent jihadist groups, they were already evident in the 1970s and 1980s, see for example the Sikh extremists discussed in Box 3.2. Alongside the ongoing threat posed by traditional military threats, many states' adversaries now come in the shape of small, widely dispersed cells. Technological developments have facilitated the

movement of potential threats and given rise to new vehicles for threatening national security – cyber attacks are a case in point. These developments mean that information relevant to the work of intelligence services is located in more physical and cyber locations, comes in more mediums, and is more fungible than ever before.

For most states, today's threat matrix is far more complex than in the past. Contemporary threats are, in many ways, more difficult subjects of intelligence collection than, for example, large, centralised Cold War adversaries. For instance, a well-placed human source inside a highly centralised state adversary may be far more useful than a source in one node of a regional/global terrorist network.

The nature and location of violent jihadist terrorist networks, in particular, has driven Western states' intelligence services to work with a range of services in the Middle East, Africa and Asia. Prior to the development of these networks, there had been limited previous contact with such services. Cooperating with these intelligence services is deemed essential in order to access necessary information and, where necessary, to intervene to counter threats. By way of example, citizens of some European states have travelled to terrorist training camps in locations such as Pakistan, Libya, Syria, and Yemen. European intelligence services have had to liaise with intelligence services in these countries in order to keep track of such individuals and, where necessary, to surveil their activities. Cooperation with so-called "non-traditional partners" has given rise to some serious problems, and it carries significant risks that will be discussed below.

BENEFITING FROM PARTNERS' COMPARATIVE ADVANTAGES

By cooperating with foreign partners, services can benefit from their partners' comparative geographical, relational, linguistic, cultural, technological, and resource advantages (or simply, differences) in information collection and analysis.[4] Most services will have some unique advantages or attributes that make cooperating with them attractive to foreign services. A good illustration was the Israeli services' unique access to Soviet Jewish émigrés coming to Israel in the 1950s and 60s. On the basis of debriefings with these immigrants, Israeli services transmitted to their US counterparts valuable information about life in the USSR from areas that US intelligence could not have accessed.[5] Although some intelligence services have global SIGINT capabilities, for some intelligence collection there is no substitute for the local knowledge, and access to buildings, government records, and networks of people that a "local" service will have. Even the largest, best resourced services are unlikely to possess the detailed knowledge of a particular country or society that may be provided by a smaller "local" service. Further, a country's geographical position, including its proximity or access to ports, airfields, and fibre optic cables is a principal reason for collaborating with its intelligence services.[6] Finally, a foreign service's technological capabilities may be highly attractive, particularly in the realm of SIGINT – this is said to be major draw for services cooperating with the NSA.[7]

Some services may also seek to benefit from a foreign partner's lower legal standards and greater "latitude" in its intelligence collection measures, for example to "outsource"

coercive interrogation (see below for further discussion). There have been suggestions that this may have been a consideration for certain Western services in the context of countering terrorism over the previous fifteen years. Now that the issue has been exposed, it is less likely that services might be attracted to cooperating with unregulated services that are not subject to oversight by independent bodies.

ALTERNATIVE PERSPECTIVES

Exchanging information and intelligence analyses with foreign partners can provide services with alternative perspectives on key issues and help them to challenge their own assumptions. Given that the intelligence world and its products are largely shielded from outside critique, the professional criticism that foreign partners can provide may be invaluable. Accordingly, services with close relationships will sometimes solicit comments on their strategic analyses. In the case of the UKUSA relationship, exchanges of analyses between services and between the UK Joint Intelligence Committee and the US National Intelligence Council and staff of the DNI have been going on for many years, providing analysts with "the equivalent of academic external examiners marking their papers."[8]

DIVISION OF LABOUR AND BURDEN SHARING

Cooperating with foreign partners can enable services to divide their labour and thus to save resources. A service can "piggyback" on a partner's information collection capacities in a particular region or of a particular type of intelligence. Close allies can work to avoid duplication of information collection efforts (e.g. Five Eyes partnership – see Box 2.3 in Chapter 2).[9] US intelligence's technological pre-eminence is long established and most allies have not sought to duplicate US SIGINT capacities. Instead, they have developed niche competencies in human intelligence (HUMINT), an area in which US intelligence has historically under-performed in many regions (relative to its size).[10] Consequently, services from smaller states have valuable HUMINT-derived insights to offer to US intelligence, while reaping the benefits of US SIGINT. A geographical division of labour is another form of burden sharing, and it has long been a key feature of the UKUSA SIGINT/COMSEC partnership (see Box 2.3 – Chapter 2). In this way, international intelligence cooperation can help ensure that "governments get better views of the world at cut prices."[11]

REDUCING RISKS ASSOCIATED WITH INTELLIGENCE COLLECTION

Cooperating with foreign partners can help services avoid engaging in high-risk intelligence collection activities. This is particularly true of HUMINT collection in volatile states and/or locations where recruiting and running agents can be extremely dangerous. It is often safer to cooperate with foreign partners whose personnel face lower risks in such contexts or partners that are simply less risk averse.[12] A good example of this would be penetrating terrorist groups whose members originate primarily from a particular ethnic or religious group. It may be easier for a service to work with a foreign partner whose intelligence officials and/or agents share these characteristics.

INTELLIGENCE TO SUPPORT MULTILATERAL POLICIES AND DECISION-MAKING

Information sharing between intelligence services within and/or with international organisations (IOs) can be highly beneficial because it helps to promote common assessments of situations and shared strategic outlooks. The EU seeks to pursue integrated common foreign, security, and defence policies. This requires the adoption of common positions in response to crises and even the deployment of military and police missions. Intelligence cooperation takes place in the INTCEN, which is intended to support situational awareness and provide early warning for the EU's External Action Service, the Council, and member states. The African Union (AU) has established a cooperation platform for the continent's intelligence services (CISSA) because it recognised "the need for more efficacious and efficient intelligence for the Peace and Security Council of the African Union in its deliberations, action and adoption of conflict prevention, management and resolution strategies."[13] In some cases, intelligence cooperation with/within IOs might be of limited professional operational significance but nonetheless a useful vehicle for buttressing political or military alliances.[14]

PROVIDING BACKCHANNELS FOR NEGOTIATIONS

Liaison with foreign intelligence services can provide a useful backchannel for discussions between two or more states, which they would prefer to keep out of the public eye and away from political processes. This has proven to be beneficial in promoting mutual understanding between states, resolving disputes, and brokering ceasefires and peace agreements. Such discussions may not always be service-to-service; in some cases, representatives of one state's intelligence services will conduct negotiations with officials from the other state's political leadership. A well-known example is the negotiations leading between Jordan and Israel in the 1990s that led to the signing of a peace treaty between the two countries.

SUPPORTING PEACEKEEPING MISSIONS AND INTERNATIONAL CRIMINAL TRIBUNALS

Information sharing by intelligence services can also benefit international peacekeeping missions by helping ensure that military commanders are aware of threats to peacekeepers, as well as on potential flashpoints for conflict. Such transfers of information are especially beneficial in contexts where international missions have very limited intelligence capabilities. Information provided by intelligence services has also played an important role in the prosecution of war criminals at international tribunals. This was particularly true of the International Criminal Tribunal for the former Yugoslavia, where persons suspected of having committed international crimes in the conflict in the former Yugoslavia were tried.[15] US military intelligence, in particular, provided crucial information that prosecutors were able to transform into evidence; this mainly consisted of geospatial intelligence.

3.3 Risks of international intelligence cooperation

International intelligence cooperation can be a high-risk area of state activity and, thus, requires careful regulation and oversight. This section will focus primarily on risks to human rights and the rule of law, but it will also discuss the risks that international intelligence cooperation can create from the point of view of the security of information, reputation, legal proceedings, and foreign relations. When thinking about the risks associated with international intelligence cooperation, it is helpful to distinguish between following broad categories of risk:

a. risks that are inherent to exchanging information or working directly with foreign intelligence services;
b. risks that are created by governments authorising their intelligence services to undertake inappropriate and/or illegal actions in collaboration with foreign intelligence services; and
c. risks that are created by intelligence services conducting covert activity without the express authorisation of their governments or knowledge of their oversight bodies.

Risks under category (a) cannot be avoided entirely and have to be managed on an ongoing basis through a combination of legislation, subsidiary regulations and internal guidelines within intelligence services; external oversight, executive stewardship of intelligence services; and internal management. It is the management of these risks that is the primary focus of this guide. Category (b) risks should not arise and can best be prevented through robust external oversight and high levels of professionalism within intelligence services, which help to resist such misuse of intelligence services. Risks under category (c) are also preventable through effective executive controls and external oversight of intelligence services, as well as appropriate legal frameworks.

Before discussing specific risk areas in international intelligence cooperation, it is worth noting several general features of international intelligence cooperation that give rise to inherent but (often) manageable risks. An axiomatic but crucial point is that intelligence services cannot control – and, at best, may have only limited influence over - what their foreign partners do as part of or as a result of cooperation. In many cases, services cannot verify what a foreign partner has done as part of or on the basis of international intelligence cooperation. Notably, they face major difficulties in verifying how a foreign service will use information sent to it, and they cannot usually ascertain how information is subsequently used. Regardless of the principle of originator control and any caveats that may be attached to outgoing information, intelligence services lose full control of information as soon as they transmit it to another body. The main constraint in practice is that violations of understandings will be sanctioned by reduction or cessation of future cooperation.

It is often very difficult for services to evaluate and validate incoming information from some foreign intelligence services. This is primarily because intelligence services are extremely protective of the sources and methods they use to gather information. Services do not readily provide such information to partners, particularly when information is derived from covert human intelligence sources. As the Dutch CTIVD has explained, “it

is generally not customary in international dealings between intelligence and security services to ask the foreign service about the source or method used to collect data, nor for the service itself to provide information about how the data was acquired."[16]

A lack of knowledge about the provenance of information has inevitable implications for assessing its reliability. The problems that can arise when the receiving service does not have direct access to a human source are well illustrated by the "Curveball" affair leading up to the Iraq war (see Box 3.1). There has also been much debate about the receipt and use of incoming information that may have been derived from torture, or inhuman and degrading treatment in violation of international human rights law. Information of this provenance is not only likely to be unreliable, but its use by a recipient raises important ethical and legal questions (the latter will explored in more detail in Chapter 4).

Box 3.1: Curveball

Rafid Alwan al-Janabi (codenamed "Curveball") was an Iraqi defector who was a key source behind US accusations that Iraq possessed WMDs in the run-up to the 2003 invasion. Curveball was a source recruited by the German Foreign Intelligence Service (BND). Over several years, he provided the BND with information about alleged Iraqi biological weapons programmes that he admitted after the war was deliberate deception in order to support the case for military intervention. The BND conveyed more than 90 intelligence reports to the US Defense Intelligence Agency (DIA) and UK intelligence, which passed them onto the CIA, which, in turn, embraced Curveball's account and used it in their assessments for policymakers. US intelligence attached great weight to the reports as being technically feasible in spite of the fact that they could not corroborate the claims, did not know who the source was, and they were not given direct access to him by the BND. German officials have subsequently stated that they transmitted clear caveats at a late stage to American intelligence about the reliability of the source, and expressed concerns to the head of the CIA in Europe at the time. The extent and nature of any warning has been disputed by the US, who allege poor tradecraft by the BND allowing Curveball to tailor his account to what was likely to have greatest impact on US assessments. Notwithstanding this debate, this affair illustrates the difficulties that can be associated with using information provided by a foreign service.[17]

Throughout the world, intelligence services operate according to very different domestic legal frameworks and divergent understandings of international law. Consequently, intelligence services in one state may be permitted to undertake activities that services in another state are precluded (by domestic and/or international law) from undertaking or contributing to. Such differences in legal approach can constitute a risk in the context of cooperation because an intelligence service may contribute to become implicated in the activities of a foreign partner, which could be deemed unlawful under the laws of its own state and (in some cases) international law.

A good example is the concerns of other Western states about cooperation with American intelligence services due to the legal positions and practices adopted by successive US administrations in their approach to counter-terrorism.[18] The US approach has been underpinned by the view that the US is engaged in (an apparently indefinite) "war" against terrorism and the concomitant rejection of a criminal-law based approach to tackling terrorism. Features of this approach have included refusing to limit the geographical boundaries in which this war paradigm applies and, despite regarding itself as being in an armed conflict, refusing full rights and protections to terrorist suspects under IHL. These legal approaches have been used to justify practices like extraordinary rendition; targeted assassination with drones outside zones of conflict, and the indefinite detention of suspected terrorists without trial. Another feature of the US approach to counter terrorism prior to 2008 was the authorisation of so-called enhanced interrogation techniques (such as waterboarding) pursuant to incorrect interpretations of internationally recognised definitions torture and inhuman and degrading treatment.

Continuing with this example, partner intelligence services, whose states follow and are bound by different definitions of torture may face legal risks regarding the sharing of information (and other forms of cooperation) relating to persons who have been subjected to such techniques and/or being involved in interrogations where such techniques were used. Similarly, an intelligence service whose state does not, for example, share the legal position that there exists a geographically unbound armed conflict with Al Qaeda and similar groups faces risks in collaboration in these circumstances because their cooperation may contribute to, for example, extrajudicial killings of suspected terrorists outside of armed conflicts (see below for further discussion).

3.4 Risks to human rights and the rule of law

International intelligence cooperation does not pose a threat to human rights per se; it can enhance protection of human rights by helping states manage serious threats to their populations. A failure to engage in and exploit the benefits of appropriate cooperation with foreign services can increase risks to human rights, particularly the right to life. The following box provides an illustration of this because of the Canadian services' failure to make effective use of information shared by Indian intelligence services contributed to their failure to prevent the bombing and thus serious loss of life.

While an absence of international intelligence cooperation can create or increase risks to human rights, it is primarily the development of closer cooperation with services and states that do not respect international legal standards has created risks to human rights. Intelligence services in non-democratic states are more likely to have a number of characteristics that make cooperating with them high risk from a human rights point of view. First, these services are not normally subject to legal regulations that comply with international standards. For example, broad mandates may give services the scope to interfere in political processes and in legitimate exercise of rights and fundamental freedoms. Effective regulations on the collection of information are unlikely to exist and services may even be permitted to detain and interrogate for the purposes of intelligence

Box 3.2: The bombing of Air India 182 and the failure to exploit international intelligence cooperation

Air India flight 182 was destroyed by a bomb in June 1985 with the loss of 329 lives. The plane was en route from Montreal to India via the UK. The bomb was planted by a Sikh militant group that was engaged in a campaign against the Indian government. The bombing was planned by members of the group living in Canada.

The Indian intelligence services had shared with their Canadian counterparts information about the existence of the group in Canada, its members, and the growing threat to various targets. It later emerged that at times Indian intelligence was "the sole source of information on the Sikh extremist threat, both within and outside Canada." An inquiry found that the Canadian services decided not to rely on the information, and they were unable to corroborate it through their own limited sources. The decision not to act on the information shared by Indian intelligence was found to be the result of there not being a long standing intelligence relationship with India, a belief that India was exaggerating the threat, and concerns that the information shared was biased. The inquiry found that not making appropriate use of shared information was one of a number of intelligence and security failures that contributed to the failure to prevent the bombing.[19]

gathering. Second, services in non-democratic states exist primarily to protect the security and interests of an incumbent regime or head of state/government. Consequently, they are often deployed against political opponents and critics of a regime exercising basic freedoms. Third, intelligence services in non-democratic states are rarely subject to independent oversight and/or judicial scrutiny. This means their activities are not subject to checks that can prevent and remedy human rights violations. Finally, such services are unlikely to have an institutional culture that promotes respect for human rights and the rule of law. Indeed, there are some services whose institutional cultures deride human rights and, for example, use torture as a standard procedure.

Indeed, this has been illustrated through the Snowden revelations about the activities of intelligence from a number of established democracies. Some well-established democracies have violated and continue to violate human rights in their intelligence work. Accordingly, the risks of cooperation cannot be discounted merely because a partner service belongs to a state that is a democracy and/or it appears to be subject to effective governance. Indeed, this has been illustrated through the Snowden revelations about the activities of intelligence from a number of so-called established democracies – examples are discussed further below. Even in the context of long-standing, close international intelligence cooperation relationships, overseers should address the question as to whether trust placed in a partner is justified.[20]

Cooperation with foreign services that have some or all of the features described above can give rise to legal, moral and reputational risks. By working with such partners, services may become implicated in or "contaminated" by their partner's human rights abuses, and they may expose themselves to accusations of collusion in or the facilitation of human

rights abuses, as well as legal proceedings. This section will provide a range of examples of how international intelligence cooperation can pose a threat to human rights.

RISKS TO HUMAN RIGHTS POSED BY INFORMATION SHARING

Sharing information with another intelligence service (and potentially retransmitting it to other authorities in that state) can have significant implications for human rights. This is primarily the case with the sharing of personal data. Such implications include entirely lawful restrictions upon an individual's rights, such as obtaining a judicial warrant to place someone under surveillance on the basis of information provided by foreign partners. Regardless of whether or not action taken on the basis of shared information is lawful, the sharing of information can have serious consequences for an individual and thus demands careful regulation and oversight. This subsection will highlight a number of examples of action that may be taken on the basis of shared information.

There have been cases, particularly in the context of counterterrorism, where a service has sent information to a foreign service knowing that the recipient may take action that violates someone's human rights. However, in most cases, the service sending the information may not anticipate, let alone request, that a particular course of action is taken by the recipient. The sending service may have attached caveats (see Chapter 6 for more on caveats) to the information to prevent the recipient using the outgoing information for certain purposes or sought assurances that, for example, if arrested a suspect will not face the death penalty. Nevertheless, the fact that a service did not intend that a foreign service would, for instance, use outgoing information to detain, render, and interrogate does not absolve them of responsibility for the possible consequences of passing on the information. In view of this, services should exercise caution and put in place risk assessment procedures, particularly when sharing information with foreign services that are known to render, arbitrarily detain, and torture persons (see Chapters 5 and 6).

Once information is shared with a foreign service, it remains with that service and, in many cases, intelligence services do not routinely destroy information held in their databases. This could potentially raise human rights concerns if the nature of the service and its government change. Change in the intelligence sector is often conceptualised as being inherently positive – reform towards democratic good governance. Yet it is possible for governments and their services to "backslide" away from a democratic system and away from respect for the rule of law and human rights. A radical change in government could, for example, lead to intelligence services using much more aggressive means to tackle individuals who are deemed to be a threat. Information shared several years previously might then suddenly serve as the basis for actions violating human rights. This theoretical risk is not manageable in practice, other than through diplomatic action with such a new regime.

The following subsections outline some of the actions that intelligence services may take (in part) on the basis of information provided by a foreign service, and how such actions

impact human rights. Our highlighting these examples is not to suggest that such actions are appropriate forms of cooperation or that they are necessarily common courses of action.

Targeted and Extrajudicial Killing

The most serious potential consequence of information sharing is its contributing to the loss of life. Targeted killings of suspected terrorists by pilotless aerial vehicles (drones) have become an increasingly common feature of US counter-terrorism policy. CIA-operated drones have been used not only in the context of an armed conflict in Afghanistan, but also in countries including Pakistan, Somalia, and Yemen. Information shared by a foreign intelligence service might in such cases be used to identify and/or locate a person who is then targeted for killing. For example, German politicians have expressed fears that information provided to American intelligence services by Germany's services may have contributed to targeted killing, including of a German citizen, in Afghanistan. Although not confirmed by the German government, concerns that outgoing information may lead to such actions have apparently caused Germany to impose stricter conditions on the sharing of personal data with US intelligence services.[21] Similar doubts have been raised in reference to the Dutch intelligence services sharing (with the US) SIGINT relating to persons in Somalia[22] and British and Australian services collecting and sharing information that may have contributed to US drone strikes in Yemen.[23] Ultimately, it may be difficult for a service sharing information (and particularly metadata) with the US to be sure that such information has not assisted in some way in the drone strikes. Providing information that could lead to killings, without due process, of persons who are not parties to an armed conflict gives rise to serious human rights concerns.

Arrest, Detention, Extraordinary Rendition and Torture

Information supplied by a foreign service may contribute to a person being detained and interrogated by an intelligence service or law enforcement body. Foreign information may enable a foreign service (or other authority) to locate a person, and it commonly serves to inform the approach that may be made if s/he is detained. Such action may be lawful if the service concerned has the legal authority to detain people, and it does so in accordance with national and international legal standards. It is not, however, regarded as good practice for intelligence services to exercise powers of arrest and detention unless they have a clear law enforcement mandate.[24] This is because detention and questioning by intelligence services carries particular risks for the people concerned as it is not normally geared towards criminal proceedings and thus lacks the supervisory and procedural safeguards that accompany such proceedings. Additionally, the use of such power by intelligence services is typically shrouded in secrecy and rarely subject to legal authorisation and oversight – detainees may have limited opportunity challenge their detention. All these actions can have weighty consequences for, *inter alia*, the rights to liberty and fair trial. Accordingly, services should pay attention to whether a foreign partner uses such powers (lawfully or otherwise) when sharing information. Detention and interrogation by services that use torture and similar techniques brings additional serious human rights consequences.

Suspected terrorists (and other perceived enemies of incumbent regimes) have sometimes been detained and interrogated following their extrajudicial transfer from another state. Transfers have frequently been carried out secretly by intelligence services, without any legal process – this practice became known as extraordinary rendition. Shared information has served as the basis for these actions (for an example of this, see Box 3.3 on Maher Arar). Extraordinary rendition has sometimes been accompanied or followed by interrogation under torture and other inhuman and degrading treatment.

Box 3.3: The case of Maher Arar

Maher Arar, a Canadian-Syrian, dual national was detained for two weeks at JFK Airport and subsequently rendered to Syria (via Jordan) by the CIA in September 2002. US authorities were acting upon intelligence shared by the Royal Canadian Mounted Police (RCMP) that was later found to be inaccurate, misleading, and without appropriate caveats – Arar and his wife were unjustifiably referred to as an "Islamic Extremist individuals suspected of being linked to the Al Qaeda terrorist movement." Syrian Military Intelligence detained Arar incommunicado for ten months and subjected him to torture. Some of this information was provided to CSIS and the RCMP; the latter used some of this information as the basis for a search warrant against Arar. Mr. Arar was eventually repatriated to Canada, where his ordeal was the subject of an extensive judicial inquiry that generated numerous lessons relevant to this policy guide.[25]

Intelligence services sometimes send specific questions to a foreign service to be addressed to persons being detained and interrogated by that service. This is especially problematic in cases where detainees have been extraordinarily rendered and/or are detained and interrogated under the conditions outlined above. Another Canadian case, that of Ahmad Abou-Elmaati, a Canadian-Egyptian, who was arbitrarily detained and tortured in Syria and Egypt, is one example of this. An inquiry found that, in addition to providing information that contributed to his detention in Syria, CSIS's sending questions to Syrian intelligence (via another foreign service) likely contributed to his mistreatment.[26] Passing questions may contribute to extended arbitrary detention and further interrogation under torture; it may also convey the message that such practices are acceptable.

Beyond sending questions to be addressed to persons in detention, there have been allegations that some Western intelligence services have requested foreign services to detain and interrogate suspected terrorists. Services making such requests do so in the expectation that information acquired from interrogation will be transmitted to them. By way of example, NGOs and media organisations have alleged that UK intelligence services to have sought the arrest and interrogation by the Pakistani intelligence services of individuals suspected of planning terrorist attacks in the UK. Various sources have claimed that British services provided information and specific questions about a number of persons in detention and then received information gleaned from these interrogations.[27] Investigations into these allegations are ongoing, with the ISC (a committee of parliamentarians) having conceded that its previous investigations of these issues were incomplete and that some information was not made available to the committee.[28]

Requesting that a person be detained, providing information leading to his/her detention, and supplying questions to be put to him/her are actions that can have significant implications for a person's human rights. Such cooperation is unlawful when a service knows (or ought to know) that the detention and interrogation methods employed by its foreign interlocutor violate human rights (see Chapter 4).

Consideration should also be given to the risk of sharing information about political opponents with services of non-democratic states whose services function primarily to preserve and protect an incumbent regime. Authoritarian states have long sought to acquire information about such persons from the services of democratic states, and particularly those whose countries are home to dissidents. The services of democratic states frequently gather information on opposition political groups and regime opponents that are part of a diaspora in their state – this is done partly to determine whether such groups pose any threat to security and potentially the relationship with their own state. In these circumstances, sharing information with the services of an authoritarian state may place persons at serious risk of being detained and mistreated if they visit or return to their country of origin (as well as the less serious risk that the information may be used to undermine freedoms engage in political activities and well as the rights to freedom of expression, association, and assembly).

SURVEILLANCE AND THE EXPLOITATION OF PERSONAL DATA

Most concerns about information sharing arise from the possibility that outgoing information may be used to detain, interrogate, and even kill people. However, shared information is more commonly used to undertake surveillance and to exploit already-collected personal data. Such surveillance may take the form of a variety of measures ranging from the placement of covert cameras and listening devices in a person's home, to the installation of malware on computers/phones, and intercepting communications. Intelligence services also use foreign information to inform their "mining" of data sets (including those held by other government departments and private companies) through the use of so-called "selectors" or key words. Beyond surveillance and the exploitation of data, foreign-supplied information may lead to some intelligence services searching premises and seizing property. Services may carry out these and other activities following a request from a foreign service or on their own initiative.

These activities normally include limitations on the right to privacy and family life of persons who are, for example, subject to surveillance or whose personal data is searched, corroborated, and examined. More indirectly, surveillance can impact upon the freedom of expression, assembly, and association. This is because persons may refrain from communicating or taking part in, for example, protest groups if they fear they are under surveillance.[29] Accordingly, the sharing of information leading to surveillance by another states intelligence services can have implications for the rights to privacy and the freedom of expression, assembly, and association.

Sharing information leading to surveillance does not necessarily give cause for concern or create any human rights risk. In most democratic countries, services generally use targeted

surveillance and other highly intrusive measures (like search and seizure) in accordance with strict legal criteria and only after receiving authorisation from an external body. Such processes can ensure that limitations on a subject's rights are lawful[30] and the sharing of information leading to the use of these measures may not give rise to concern. By contrast, in many non-democratic states' intelligence services, surveillance is not governed by proper legal frameworks or subject to appropriate safeguards. With this in mind, sharing information that may lead to surveillance, search and seizure, or other exploitation of personal data can pose a risk to the human rights of persons concerned. Finally, given that the Snowden revelations have demonstrated that in many countries (including established democracies) untargeted surveillance is not undertaken in a manner that complies with human rights law, it may also be said that sharing information that leads or contributes to these activities also contributes to a risk to human rights.

IMMIGRATION MEASURES

Information provided by foreign services is very frequently used in decisions relating to immigration and asylum. Intelligence services often play a role in security screening in the context of, for example, decisions on the entry of foreigners, visa and asylum applications, and the deportation of foreigners. Such determinations can have consequences for an individual's liberty, freedom of movement, the right to privacy and a family life, and, if a person is deported, the right to life and the right not to be subject to torture. A good example is that of Ahmed Zaoui in New Zealand (see Box 3.4).

Box 3.4: The case of Ahmed Zaoui

Ahmed Zaoui is former Algerian parliamentarian who claimed asylum upon arriving in New Zealand (NZ) in December 2002. He was denied asylum and held in administrative detention for almost two years on the basis of a security risk certificate issued by NZSIS. The service issued the certificate on the basis of information received from various foreign intelligence services, which the NZSIS interpreted as showing that Zaoui was a threat to national security. This information related to his activities in Europe, as a member of an Algerian opposition group, after fleeing Algeria following the military coup of 1991. NZSIS is alleged to have interpreted foreign information selectively. Because the information came from foreign services, it was extremely difficult for Zaoui to challenge; the NZSIS argued that much of the information underpinning the security risk certificate could not be revealed because it would harm their relations with foreign services. After protracted legal proceedings Zaoui was released on bail and NZSIS withdrew the security risk certificate. He has now settled in New Zealand.[31]

Targeted Sanctions

Also in the context of counter-terrorism, intelligence services play a pre-eminent role in supplying information that is used as the basis for targeted sanctions (primarily) against suspected terrorists. Sanctions include the freezing of financial assets, denial of access to markers and travel restrictions; they are intended to "contain" persons deemed to pose a threat. Some states unilaterally impose targeted sanctions, but they are more commonly instituted by the UNSC and regional bodies like the EU. Multilateral bodies rely extensively on states' intelligence services to provide information on relevant persons. These measures have quasi-punitive results and significant implications for the rights to liberty and freedom of movement, assembly, association and expression. The weight of such consequences is exacerbated by the fact that it remains extremely difficult for individuals and groups to challenge their listing.[32] It is, therefore, extremely important that states have robust procedures for themselves to validate intelligence for such purposes before it is passed on.

DIRECT INVOLVEMENT IN JOINT OPERATIONS THAT VIOLATE HUMAN RIGHTS

As was discussed in Chapter 2, international intelligence cooperation goes beyond information sharing. Other forms of cooperation can also pose a significant risk to human rights; many of these forms of cooperation entail direct involvement in the actions taken on the basis of shared information.

Direct Involvement in Extraordinary Rendition

A number of intelligence services have been directly involved in US intelligence-led abduction, detention, and rendering of suspected terrorists. Examples include the cases of Abu Omar and Khaled El Masri. Italian intelligence service officers worked with American intelligence officials to abduct Abu Omar from the streets of Milan; he was subsequently rendered to Egypt (by the CIA) where he detained extra-judicially for 14 months and subjected to torture.[33] Macedonian security services acted alone in arresting and detaining El-Masri *incommunicado* in a hotel for 23 days before transferring him to the custody of the CIA at Skopje airport, where he was severely abused in front of Macedonian agents. He was rendered to Afghanistan where he was detained and tortured for four months.[34]

Interrogation

There are situations in which services request permission to question persons in the custody or other states intelligence service or police. Such interrogations do not pose an inherent threat to human rights if the persons concerned are being held lawfully and treated in accordance with international standards. However, if members of an intelligence service interrogate (either alone or in collaboration with the detaining entity) someone who is being detained unlawfully and/or subject to torture by a foreign entity, this may exacerbate the risk to the individual concerned.[35] Undertaking interrogations in such contexts and failing to take action to stop violations by the service holding the person may also give rise to liability on the part the service and its employees (see Chapter 4).

COOPERATION TO CIRCUMVENT NATIONAL LEGAL REGULATIONS AND OVERSIGHT PROCESSES: FOLLOWING THE ROAD OF LEAST ACCOUNTABILITY

There is a risk that international intelligence cooperation may be used to circumvent (or inadvertently cause to be circumvented) national laws regulating intelligence services and/or oversight arrangements. This subsection discusses a number of ways in which this may occur. Given the increasing importance of international intelligence cooperation, this is a risk to which legislators, members of the executive, and overseers should be particularly alert.

Cooperating with Foreign Partners to Obtain Information that could not be Lawfully Obtained

Information sharing is the main area of international intelligence cooperation that risks bypassing national laws and safeguards on the collection of information – some intelligence services may engage in what has been labelled "collusion for circumvention."[36] Consequently, there have long been suggestions that some services have used their relationships with foreign partners to access information that they either could not lawfully obtain themselves or would be difficult from them to obtain lawfully. This may be the case for a variety of reasons, including a would-be target's status as a citizen of the state concerned (in circumstances where a service is not permitted to gather information on its state's own citizens); the fact that the actions of a person of interest have not met a requisite threshold of suspicion; the activities in which a would-be target is involved cannot be investigated by the service under the relevant legislation governing the service; a would-be target's membership of a profession that is protected (e.g. a member of parliament); or legal restrictions on using particular methods to collect information. Faced with these difficulties, some intelligence services may turn to foreign partners to acquire the information sought. Such information may be (a) provided from information already collected by a foreign partner or (b) following further surveillance by a foreign partner – both situations are discussed below.

In 2014, the UN High Commissioner for Human Rights expressed concerns that there is:

> credible information to suggest that some Governments systematically have routed data collection and analytical tasks through jurisdictions with weaker safeguards for privacy. Reportedly, some Governments have operated a transnational network of intelligence agencies through interlocking legal loopholes, involving the coordination of surveillance practice to outflank the protections provided by domestic legal regimes.[37]

Revelations by Edward Snowden (hitherto denied by the UK government and its oversight bodies[38]) have given rise to concerns that Britain's GCHQ and the NSA may exploit their relationship to acquire information that would be more difficult to obtain lawfully themselves, within their own jurisdictions.[39] Indications that US intelligence may regard the UK legal framework for surveillance as more permissive than their own illustrate the potential attractiveness of international intelligence cooperation for sidestepping domestic constraints on surveillance.[40] Conversely, documents disclosed in the context

of litigation against GCHQ and other defendants appear to indicate that UK intelligence services have been permitted, by an internal policy, to access (without a warrant) bulk data intercepted through NSA SIGINT activities, even though GCHQ would require a warrant in order to acquire such information itself.[41] Similar concerns (also denied) have been raised with respect to BND-NSA cooperation in Germany. The German constitution prohibits the BND from conducting surveillance against German citizens, but it is alleged that in its close cooperation with the NSA (including through jointly operated surveillance facilities) it has received information on German citizens (see Box 2.2 in Chapter 2).[42]

Beyond the sharing of information that has already been collected by a foreign partner, some intelligence services may request a foreign service to conduct surveillance on its territory or turn a blind eye to such surveillance by a foreign partner in the knowledge that they will receive the information collected. This is alleged to have occurred amongst some EU states.[43] When a foreign partner service conducts surveillance on a state's territory, it would ordinarily have to obtain the permission of the local service, which would assume a level of responsibility for any operation and would presumably receive the information collected. Any such collection should comply with the host state's own laws on surveillance. Alternatively, a service may request a foreign service to place one its citizens overseas under surveillance whom it would not be permitted by the law to surveil. For example, New Zealand's GCSB (a signals intelligence service) is not currently permitted to surveil New Zealanders. Yet it is alleged to have asked the NSA to intercept the phone calls of an NZ journalist in Afghanistan in order to uncover his confidential sources that were behind stories on the NZ military's handling of detainees.[44]

There is an important difference between, on the one hand, an intelligence service asking a foreign partner for information or deliberately accessing it from a partner's databases and, on the other hand, receiving it without having requested it. Requests to a foreign service to collect information or provide information already in its possession on particular persons can be regulated and subject to appropriate authorisation procedures, as can the exercise of any power to access directly a foreign partner's databases. If a service could not lawfully collect, access, or retain particular information themselves, it is clear that they should not be permitted to circumvent this by requesting the information from a foreign partner. A greater regulatory (and oversight) challenge arises with regards to information that is passively received without an explicit request. Such sharing may occur whenever a liaison partner acquires intelligence bearing on the security of a partner state; this is particularly common between services whose countries have very close relationships.[45] It may even happen automatically within a highly integrated signals intelligence sharing relationship like the Five Eyes partnership (see Box 2.3 in Chapter 2). Consideration should be given to how procedures can be put in place to ensure that the receipt of such information does not lead to *de facto* bypassing of national law on information collection by the recipient service (see Chapters 5 and 6 for further discussion).

In addition to circumvention of domestic legal standards and safeguards in obtaining information, concerns have been raised that collusion for circumvention has also included services providing advice to partners on how to weaken or reinterpret domestic regulations on information gathering to facilitate more expansive surveillance.[46] It is likely that such

advice would be provided in the knowledge that a foreign partner facing fewer barriers to surveillance is likely to gather information which can then be shared.

Outsourcing Coercive Interrogation

Intelligence cooperation relationships have been used to exploit foreign services' propensity for using unlawful conditions of detention and coercive interrogation to extract information from persons of interest. This was a significant purpose of the US-led extraordinary rendition programme that included suspected terrorists being rendered to the custody of and interrogated by intelligence services known for their use of coercive interrogation.[47] In some cases, the persons concerned had no connection to the countries into whose custody they were transferred. Even where services have not been directly involved in rendering a person to the custody of a foreign service, they may have facilitated the apprehension and detention of persons (including their own citizens) by foreign services.

Working With Foreign Services To Establish Facilities In Areas Of Limited Oversight

As part of the aforementioned programme of extraordinary rendition and arbitrary detention, US services worked with some foreign services to create secret detention and interrogation facilities. A process of "jurisdiction shopping" appears to have taken place. These facilities were generally set up in states where oversight bodies and other sources of scrutiny either didn't exist or would be unlikely to uncover activities.[48] Setting up facilities abroad also ensured that they were beyond the likely reach of US courts and oversight authorities.

REPUTATIONAL AND LEGAL RISKS

International intelligence cooperation can present legal and reputational risks for services, their personnel, and their governments. Governments are ultimately responsible for their intelligence services, and international intelligence cooperation is an area of intelligence work that can have political consequences domestically and internationally. By way of example, international intelligence cooperation-related disclosures made by Edward Snowden caused embarrassment to the German government in the run up to the 2013 election. It was alleged that Germany's intelligence services have worked closely with US intelligence on surveillance initiatives while the government publicly admonished the Americans following the wider Snowden revelations on surveillance.[49] Further embarrassment followed when documents disclosed by Snowden indicated that the BND (Germany's foreign intelligence service) has carried out SIGINT collection against European targets (including companies and politicians) on behalf of the NSA (see Box 2.2 in Chapter 2).[50]

The presence of such reputational risks demands that services consider potential damage, consult with ministers, and seek authorisation where appropriate when entering or extending relationships with foreign partners and when engaging in specific instances of cooperation with any foreign service. This is particularly important for covert operational

cooperation, including situations where services permit foreign partners to conduct activities on their territory.[51] Services' internal guidelines should require the consideration of such risks (see Chapter 6). Given the potential political consequences of intelligence cooperation, appropriate executive oversight of international intelligence cooperation is essential (see Chapter 6).

Governments also need to be mindful of the potential state legal responsibility arising from international intelligence cooperation. Victims of the US-led rendition and secret detention programme have brought claims against several European states for their involvement in these activities. The European Court of Human Rights has ruled against Macedonia, for its role in the detention, torture and extradition rendition of Khaled El Masri by the CIA, and Poland, for its role in the CIA's rendition, secret detention and mistreatment of Al Nashiri and Abu Zubaydah in Poland. Decisions are pending in cases brought against Romania (Al Nashiri), Italy (Nasr/Abu Omar) and Lithuania (Abu Zubaydah), which also relate to the CIA extraordinary rendition and secret detention programme.[52] Chapter 4 provides a further discussion on these cases and on the international legal rules on state responsibility as they apply to international intelligence cooperation.

Within intelligence services, concerns have grown about personal criminal liability for involvement in aspects of international intelligence cooperation. Although there have been few prosecutions for international intelligence cooperation-related activities, in Italy 23 American officials were convicted (*in absentia*) and five former Italian military intelligence service officials convicted and imprisoned for their role in the abduction of Abu Omar. The Italians' convictions were later overturned on complex grounds relating to state secrets.[53] The issue of criminal liability arises not only in cases where services have participated in activities that are unambiguously illegal, such as abduction or torture, but also with regards to information sharing. Sharing information that leads to, for instance, serious human rights abuse may, in some circumstances, engage criminal responsibility of the persons involved (see Chapter 4). Given the potential for criminal liability arising from international intelligence cooperation, training on compliance with legal standards, clear internal guidelines on cooperation and designated channels for raising concerns are especially important (see Chapter 6).

SECURITY RISKS

Sharing information with foreign intelligence services carries an inherent security risk. There are myriad ways that the information could be misused. Examples include the exploitation of the information in ways that could jeopardise the source, inadvertent unauthorised disclosure of the information due to lax security procedures, disclosing the information in a public forum, deliberately passing on the information to a third foreign service, or a "mole" could pass the information to a hostile service.[54]

The misuse of shared information by a foreign service or one its members of staff can have serious implications for the sending service's personnel, sources, and methods. In the worst cases, it could lead the loss of life or major financial loss inflicted by the need to alter, for example, IT systems or collection methods. The misuse of information received

from a foreign service can also do serious harm to a service's reputation as a cooperation partner and, ultimately, to a state's security if potentially vital information is no longer shared.[55] It is essential to stress, however, that legitimate disclosures of information in order to comply with oversight requirements within "the circle of secrecy" or domestic legal processes should not to be conceptualised as the misuse of information or an inherent security risk, provided that appropriate security measures are in place.

Engaging with foreign intelligence services also creates the risk (or opportunity) of espionage. Services may try to recruit their foreign interlocutors as sources. One former senior CIA official has suggested that CIA instructors taught that "liaison existed for one primary purpose: to gain access to these foreign services and recruit sources within their ranks" – this is described as the "liaison-for-spying doctrine."[56] Having sources within another service may facilitate much greater access to information than would ordinarily be available through information exchanges. While this represents a concern for any service, the benefits of cooperation are generally seen to outweigh such risks.

POSSIBLE MANIPULATION AND UNDUE INFLUENCE BY FOREIGN SERVICES

Most governments and intelligence services would like partners to share their outlooks on the world, including strategic priorities and perceptions of threat. Intelligence cooperation can be an important means of promoting this. The use of information sharing to shape another state's perceptions of threats may be seen as a benefit of cooperation. This is particularly beneficial if it is used to persuade a partner to not to take precipitate action and avoid conflicts.

However, cooperation with foreign services also gives rise to the risk that intelligence services and their governments may be manipulated by foreign partners. Using intelligence cooperation to shape or manipulate another state's perceptions and decisions can be attempted through (sometimes selective) sharing of information, analyses and even sources.[57] Such aims can also be pursued more subtly through other forms of cooperation such as training in operational techniques, contributions to drafting laws, and the provision of equipment. Powerful states and their services place considerable pressure on partners to adopt their security concerns. For example, states affected by jihadist terrorism have sought to promote this as a priority for partner services even where terrorism is not a pre-eminent threat to the security of their partners. Former senior South African intelligence official, Barry Gilder, provides a useful insight into to how such priorities can be foisted upon a service. Discussing the 2000 Cape Town bombing, Gilder explains, "[T]he Western intelligence services jumped on the […] bombings with gusto […] They (the Americans) offered us all manner of assistance – equipment, money, training, expertise. They insisted there must be a link to international terrorism. We found none."[58] A further example was revealed in leaked documents from South Africa in 2015, which suggest that, under pressure from US and other Western intelligence services, the National Intelligence Agency (NIA) devoted considerable resources to gathering intelligence on Iranian agents and intentions in South Africa. This was done in spite of the fact that the NIA did not consider Iran and its agents to be a significant security threat.[59]

Although considerable intelligence benefits may be derived from two or more services specialising in the collection of information of particular issues/geographical areas/groups and sharing their results, there is a risk that an intelligence service's information collection activities may come to be defined by the requirements of a foreign partner. This is most likely to arise in highly asymmetrical intelligence relationships, where a service is dependent on a foreign partner and/or beholden to a foreign partner by virtue of, for example, that partner service having provided funding, equipment and training. Indeed, some international intelligence cooperation relationships may become customer-client relationships.[60] In such situations, services may focus upon (and expend resources) seeking to meet the requirements of a foreign service to ensure ongoing support or due to diplomatic pressure, rather than addressing priorities that are more relevant to its country. This may come at the expense of focusing on issues that have been identified as priorities by elected officials and, in some states, legislatures. By way of example, it has been reported that Germany's BND became more independent of its own government and fell increasingly under the influence of US intelligence following an intensification of cooperation with the NSA in the early 2000s.[61] With all of these concerns in mind, intelligence cooperation must be "carefully managed to ensure it properly reflects the policies of the respective governments [and] that intelligence security concerns are indeed mutually shared" (see Chapter 6 on the role of the executive in this area).[62]

RISKS TO FOREIGN POLICY

Intelligence cooperation is commonly aligned with and in support of a state's foreign policy objectives. It is possible that relationships with foreign services could undermine foreign policy if a service's professional aspirations are not consistent with executive policy. For instance, sharing information with a particular foreign service might bring benefits from a service's point of view but contradict government policy not to engage with a particular state due to, for example, its domestic policy or human rights record. The potential for such inconsistencies (and their consequences) demands that the executive branch supervises its services' foreign relationships and intervenes where necessary.

Endnotes

1. Michael Herman, *Intelligence power in peace and war*, (Cambridge: Cambridge University Press, 1996), 204; Jennifer Sims, "Foreign Intelligence Liaison: Devils, Deals, and Details," *International Journal of Intelligence and Counterintelligence* 19, (2006): 203.
2. See for example: "Africa's Jihadists, on their way," *The Economist*, 26 July 2014.
3. Cited in Ian Cobain, *Cruel Britannia, A Secret History of Torture*, (London: Portobello Books, 2012), 236; Sims, "Foreign Intelligence Liaison: Devils, Deals, and Details," 203.
4. See for example: US, National Security Agency, *What Are We After with Our Third Party Relationships? — And What Do They Want from Us, Generally Speaking? The Intercept*, 13 March 2014.
5. Ephraim Kahana, "Mossad-CIA Cooperation," *International Journal of Intelligence and Counterintelligence* 14, (2001): 410-11.
6. See for example: Herman, *Intelligence power in peace and war*, 204-205; Ryan Gallagher, "How Secret Partners Expand NSA's Surveillance Dragnet," *The Intercept*, 19 June 2014.
7. US, National Security Agency, *What Are We After with Our Third Party Relationships?*
8. Herman, *Intelligence power in peace and war*, 209; Rhodri Jeffreys-Jones, *In Spies We Trust: The Story of Western Intelligence*, (Oxford: OUP, 2013), 189; Martin Rudner, "Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism," *International Journal of Intelligence and Counterintelligence* 17 (2004): 213; Stephen Lander, "International Intelligence Cooperation: An Inside Perspective," *Review of International Affairs*, vol. 17 no. 3, (2007): 491.
9. Jeffreys-Jones, *In Spies We Trust*, 103-104.
10. Sims, "Foreign Intelligence Liaison: Devils, Deals, and Details," 203.
11. Herman, *Intelligence power in peace and war*, 211.
12. Sims, "Foreign Intelligence Liaison: Devils, Deals, and Details," 203.
13. "The Objectives of CISSA," *Committee of Intelligence and Security Services of Africa (CISSA)*, http://cissaau.org/about-cissa/objectives.
14. Sims, "Foreign Intelligence Liaison: Devils, Deals, and Details," 202.
15. Simon Chesterman, "Intelligence cooperation in international operations," in *International Intelligence Cooperation and Accountability*, ed., Hans Born, Ian Leigh and Aidan Wills (London: Routledge, 2011), 138-141.
16. Netherlands, Review Committee on the Intelligence and Security Services, *Review Report on the Processing of Telecommunications Data by GISS and DISS*, Review Report no. 38, (The Hague, 2014), 28.
17. Bob Drogin and John Goetz, "How U.S. Fell under the Spell of 'Curveball'," *Los Angeles Times*, 20 November 2005; Martin Churlov and Helen Pidd, "Curveball: How US was duped by Iraqi fantasist," *The Guardian*, 15 February 2011; Joby Warrick, "Warnings on WMD Fabricator Were Ignored: Ex-CIA Aide Says," *Washington Post*, 25 June 2006.
18. See for example: UK, *Report of the Detainee Inquiry*, (London: HM Stationery Office, 2013), 26-27.
19. Canada, Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Air India: A Canadian Tragedy*, Volume 2, (Ottawa: Public Works and Government Services Canada, 2010), 422-431.
20. See for example: Netherlands, Review Committee on the Intelligence and Security Services, *Review Report on the Processing of Telecommunications Data by GISS and DISS*, 29.
21. Holger Stark, "Germany Limits Information Exchange with US Intelligence," *Der Spiegel*, 17 May 2011; Louise Osborne, "Germany denies phone data sent to NSA used in drone attacks," *The Guardian*, 12 August 2013.
22. Amrit Singh, *Death by Drone*, (New York: Open Society Foundation, 2015), 35-38.
23. Alice Ross and James Ball, "GCHQ documents raise fresh questions over UK complicity in US drone strikes," *The Guardian*, 24 June 2015.
24. UN Special Rapporteur on Human Rights and Counterterrorism, *Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*, A/HRC/14/46, May 2010, Practices 27-29.
25. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Ara: Analysis and Recommendations*, (Ottawa: Canadian Government Publishing, 2006), 13-15; Open Society Justice Initiative, *Globalizing Torture*, (New York: OSF, 2013), 32.
26. Justice Frank Iacobucci (Commissioner), *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin*, (Ottawa: 2008), 345-366.

27. Human Rights Watch, *Cruel Britannia, British Complicity in the Torture and Ill-Treatment of Terror Suspects in Pakistan*, 24 November 2009; Cobain, *Cruel Britannia*, 240-242, 253, 257-258.
28. UK, Intelligence and Security Committee, Press release, "Detainee Inquiry," 19 December 2013; See also: UK, *Report of the Detainee Inquiry*, 22-29.
29. See further: Commissioner for Human Rights of the Council of Europe, *Democratic and effective oversight of national security services*, Issue paper (Strasbourg: May 2015), 25-26.
30. For an overview see: Lauren Hutton, "Overseeing Information Collection," in *Overseeing Intelligence Services: A Toolkit*, ed., Hans Born and Aidan Wills, (Geneva: DCAF, 2012), 93-100.
31. Gordon Campbell, "Zaoui – The Final Chapter?" *Scoop.co.nz*, 14 September 2007; Gordon Campbell, "The Zaoui Case – Injustice on the Cheap," *Scoop.co.nz*, 16 July 2007; "SIS Summary of allegations against Ahmed Zaoui," *New Zealand Herald*, 20 February 2004; Sharon Lundy, "The Zaoui Story," *New Zealand Herald*, 13 September 2007.
32. Iain Cameron, "Blacklisting and Financial Sanctions Against Suspected Terrorists," in *International Intelligence Cooperation and Accountability*, 45-46, 49-54, 61-65.
33. Open Society Justice Initiative, *Globalizing Torture: CIA Secret Detention and Extraordinary Rendition*, (New York: OSF, 2013), 51.
34. *El Masri v. the Former Yugoslav Republic of Macedonia*, ECHR, 39630/09, 13 December 2012, paras. 149-166, 200-211; Open Society Justice Initiative, *Globalizing Torture*, 48.
35. For a discussion of these issues in relation to UK intelligence services' collaboration with foreign services, see: UK, *Report of the Detainee Inquiry*, 24-29; Human Rights Watch, *Cruel Britannia, British Complicity in the Torture and Ill-Treatment of Terror Suspects in Pakistan*, 24 November 2009; Cobain, *Cruel Britannia*, 240-242, 253, 257-258.
36. Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe (Rapporteur Pieter Omtzigt), *Mass Surveillance*, paras 30-31.
37. United Nations High Commissioner for Human Rights, *The Right to Privacy in a Digital Age*, A/HRC/27/37, 30 June 2014, para 30.
38. UK, Interception of Communications Commissioner, 2013 *Annual Report of the Interception of Communications Commissioner*, HC 1184 (April 2014), 62; UK, Intelligence and Security Committee, *Statement on GCHQ's Alleged Interception of Communications Under the US PRISM Programme*, 17 July 2013.
39. UK Hansard, 10 June 2013, Cols. 34, 35 and 39; Patrick Wintour, "David Blunkett calls for tighter scrutiny of British secret services," *The Guardian*, 10 June 2013; Richard Norton-Taylor and Nick Hopkins, "Intelligence-gathering by British state out of control, Defence and Security Blog," *The Guardian*, 11 June 2013.
40. Nick Hopkins and Spencer Ackermann, "Flexible laws and weak oversight give GCHQ room for manoeuvre," *The Guardian*, 2 August 2013.
41. "Secret policy reveals GCHQ can get warrantless access to bulk NSA data," *Privacy International*, 28 October 2014; Eric King, "Snowden vindicated: The truth about raw intelligence sharing," *Privacy International*, 29 October 2014.
42. "Spying Together: Germany's Deep Cooperation with the NSA," *Der Spiegel*, 18 June 2014.
43. Bjorn Muller-Wille, "Improving Democratic Accountability of EU Intelligence," *Intelligence and National Security* 21, No. 1 (2006): 108; European Parliament, *Report on Echelon*, A5-0264/2001, 11 July 2001, 72.
44. Nicky Hager, "US spy agencies eavesdrop on Kiwi," *Stuff.co.nz*, 28 July 2013.
45. For example, US-UK intelligence sharing discussed in: "Fighting Terror With Torture," *BBC Panorama*, first broadcast on Monday 3 August 2015.
46. See for example: Andrew Bryne, "Snowden: US spy agencies pressed EU states to ease privacy laws," *Financial Times*, 7 March 2014.
47. See generally: Open Society Justice Initiative, *Globalizing Torture: CIA Secret Detention and Extraordinary Rendition*.
48. For an overview see: Parliamentary Assembly of the Council of Europe Legal Affairs and Human Rights Committee (Rapporteur Dick Marty), *Secret detentions and illegal transfers of detainees involving Council of Europe member states: second report*, Doc. 11302 rev, June 2007; Open Society Justice Initiative, *Globalizing Torture*.
49. Rene Pfister et al. "Secret Links Between Germany and the NSA." *Der Spiegel*, 22 July 2009.
50. "America's Willing Helper: Intelligence Scandal Puts Merkel in Tight Place," *Der Spiegel*, 4 May 2015; Michel Sauga et al., "'Secrets Must Remain Secret': German Intelligence Coordinator on NSA and Media Leaks," *Der Spiegel*, 14 August 2015.
51. Henry Crumpton, *The Art of Intelligence: Lessons from a Life in the CIA's Clandestine Service*, (New York: Penguin, 2012), 90.

52. *El-Masri v. The Former Yugoslav Republic of Macedonia*, no. 39630/09, 13 December 2012; *Al Nashiri v. Poland*, no. 28761/11, 24 July 2014; European Court of Human Rights, *Secret Detention Factsheet*, June 2015.
53. See further: Yasha Maccanico, "State Secrets in the Abu Omar Case," *Statewatch*, August 2014.
54. Herman, *Intelligence power in peace and war*, 208-209.
55. Elizabeth Sepper, "Democracy, Human Rights and Intelligence Sharing," *Texas International Law Journal* 46 (2010): 165.
56. Crumpton, *The Art of Intelligence*, 84; Barry Gilder, *Songs and Secrets: South Africa from Liberation to Governance*, (London: Hurst, 2012), 212; Sims, "Foreign Intelligence Liaison: Devils, Deals, and Details," 205.
57. Sims, "Foreign Intelligence Liaison: Devils, Deals, and Details," 196.
58. Gilder, *Songs and Secrets*, 204, 165, 180; Rudner, "Hunters and Gatherers," 213.
59. Seumas Milne and Ewen MacAskill, "South Africa monitored Iranian agents under US pressure, spy cables show," *The Guardian*, 23 February 2015.
60. Herman, *Intelligence power in peace and war*, 211-212.
61. "America's Willing Helper: Intelligence Scandal Puts Merkel in Tight Place," *Der Spiegel*, 4 May 2015.
62. Gilder, *Songs and Secrets*, 212.

Part II: Legal Frameworks of International Intelligence Cooperation

4

International Legal Standards and International Intelligence Cooperation

4.1 Introduction

The purpose of this chapter is to outline the ways in which international law applies to international intelligence cooperation. It is intended to assist those advising about cooperation or responsible for its oversight by explaining the international legal parameters within which it operates. It also counters the misconception that international intelligence cooperation takes places in a legal vacuum where intelligence services operate with impunity.

The chapter first discusses the international legal basis for international intelligence cooperation. It then analyses various types of international intelligence cooperation and the application of international law to them, before focusing on specific international legal standards applicable to some forms of cooperation. It concludes by examining the duty to cooperate with international investigations and legal proceedings in the event of alleged breach of international law.

International law is relevant to international intelligence cooperation in several ways. At a strategic level, intelligence cooperation between states is sometimes based upon treaty agreements (whether bilaterally or multilaterally) or on other agreements which are secret. More commonly, it is based upon "non-treaty agreements," which are strictly

not legally binding. At the policy and operational levels of cooperation, the responsibility of the state in international law follows from the fact that intelligence services are organs of the state, and intelligence officers are state officials whose actions (and omissions) are therefore attributable to the state.[1] In the words of the UN Committee Against Torture, "intelligence activities, notwithstanding their author, nature or location, are acts of the State party, fully engaging its international responsibility."[2] The actions of officials are attributable to the state even if the individual official was acting contrary to instructions or beyond their authority.[3] Moreover, intelligence officials may also incur personal liability for their actions under international criminal law, and this possibility has led services and personnel to become more risk averse and, consequently, to greater recourse to legal advice. Similarly, the state may be liable for the actions of contractors who do not form part of its security services, where acting on the instructions, or under the direction and control, of the state.[4]

As discussed below, responsibility may arise *directly* through the wrongful actions of the services or officials that violate another state's sovereignty or human rights norms, or *indirectly* where a state is complicit in or assists the wrongful actions of its intelligence partners. In practice, one of the most pressing concerns for accountability of international intelligence cooperation from an international perspective is the question of indirect or secondary liability arising from use of executive and legal processes (for example, deportation or prosecution) based on information derived from partners, especially where there is a possibility that it may be derived from torture. This is discussed more fully in section 4.3 below.

Intelligence cooperation is not confined to exchanges or liaison between states, however. Intelligence may also be shared between states and international organisations or their subsidiary bodies responsible for peacekeeping operations, anti-terrorism measures, non-proliferation or detection, and prosecution of war criminals. In such cases, both the state and the international organisation are responsible for actions based on cooperation, such as blacklisting (See Sections 4.2 and 4.3 below).

4.2 International legal basis for international intelligence cooperation

This section outlines the relevance of the main sources of international law for international intelligence cooperation: bi-lateral cooperation, multi-lateral treaties, and the law on state responsibility.

BI-LATERAL COOPERATION

As we have seen in Chapter 2, much intelligence cooperation rests on bilateral arrangements between services acting on behalf of states. At this level agreements are likely to be general in nature. Although, in theory, some of these agreements may have the characteristics of treaties (since they are international agreements between sovereign states in written form),[5] they are usually nonetheless secret. Without registration with the

Secretariat of the United Nations, as required by Article 102 of the UN Charter, a treaty is not enforceable. More commonly, however, the partners make clear that they do not intend to be governed by international law and use a format such as a memorandum of understanding to express the terms of their agreement.[6]

A recently released example is the *Memorandum of Understanding between the National Security Agency/ Central Security Service and the Israeli SIGINT National Unit Pertaining to the Protection of U.S. Persons* the purpose of which is described in Box 4.1.

Box 4.1: US-Israel SIGINT memorandum[7]

"This agreement between NSA and The Israeli SIGINT National Unit (ISNU) prescribes procedures and responsibilities for ensuring that ISNU handling of materials provided by NSA - including, but not limited to, Signals Intelligence (SIGINT) technology and equipment and raw SIGINT data signals (i.e., intelligence information that has not been reviewed for foreign intelligence purposes or minimized) -is consistent with the requirements placed upon NSA by U.S. law and Executive Order to establish safeguards protecting the rights of U.S. persons under the Fourth Amendment to the United States Constitution.

- This agreement will apply to any SIGINT raw traffic, technology, or enabling that NSA may provide to ISNU. This agreement applies only to materials provided by NSA and shall not be construed to apply to materials collected independently by ISNU.
- ISNU also recognizes that NSA has agreements with Australia, Canada, New Zealand, and the United Kingdom that require it to protect information associated with UK persons, Australian persons, Canadian persons and New Zealand persons using procedures and safeguards similar to those applied for U.S. persons. For this reason, in all uses of raw material provided by NSA, ISNU agrees to apply the procedures outlined in this agreement to persons of these countries.
- This agreement is not intended to create any legally enforceable rights and shall not be construed to be either an international agreement or a legally binding instrument according to international law."

The use of non-treaty arrangements protects the secrecy of cooperation. It also means that formal procedures governing treaties will not apply, such as the obligation to register the agreement and constitutional procedures for democratic approval prior to ratification. One consequence is that there is less opportunity for scrutiny and accountability concerning these arrangements. The lack of an intention to create a legally binding agreement does not, however, affect a state's responsibility in international law to third parties (whether to states or affected individuals) for any actions at the tactical or operational levels in implementing the arrangements. These considerations make it all the more important that provision is made in domestic law for political approval and for oversight of cooperation arrangements, as discussed in Chapters 5, 6 and 7.

Bilateral relations may also be governed by Status of Forces Agreements in the case of military installations or bases of a partner state hosted in a state's territory. Some of these

installations, especially in the field of signals intelligence, are wholly or mainly devoted to intelligence-gathering activities. The geographical location may give the intelligence service, which is being hosted on another state's territory, proximity to regions of strategic interest or access to significant communications resources/facilities (for example, communications cables).[8] The intelligence gathered may be shared with the host state, or there may be some other *quid pro quo* (see Chapter 2).

MULTI-LATERAL COOPERATION

In addition to bilateral international intelligence cooperation, recent decades have seen a growth in treaty-based multi-lateral cooperation.[9] States routinely cooperate, for example, in the exchange of financial or air passenger information, or through EUROPOL (the European Union's law enforcement agency) or EU INTCEN (the European Union Intelligence Analysis Centre), as well as in the apprehension and prosecution of terrorists through extradition. Over-arching legal arrangements for cooperation exist at multiple levels, under UN Resolution 1373, within the Council of Europe, and under the NATO Treaty. Similarly, some cooperation is for the purpose of enforcing international legal operations or regimes such as international peacekeeping, sanctions and terrorist blacklisting,[10] arms control and non-proliferation, and international criminal law.[11]

Foremost among these is UN Security Council Resolution 1373,[12] passed in response to the attacks of 11 September 2001. This Resolution requires states to take action against everyone who commits or attempts to commit terrorist acts or facilitates their commission. The preamble recognised the need for states to complement international cooperation by taking additional measures to prevent and suppress, through all lawful means, the financing and preparation of any acts of terrorism. It, therefore, required states to take a series of measures against terrorism financing and those involved in it.

Box 4.2: UN Security Council Resolution 1373

The resolution called upon all states to "find ways of intensifying and accelerating the exchange of operational information", to "exchange information in accordance with international and domestic law (…) to prevent the commission of terrorist acts" and to "cooperate, particularly through bilateral and multilateral arrangements and agreements, to prevent and suppress terrorist attacks and take action against perpetrators of such acts.[13]

Under the Resolution all states shall:

- Prevent and suppress the financing of terrorist acts;
- Criminalize the wilful provision or collection ... of funds by their nationals or in their territories with the intention that the funds should be used ... to carry out terrorist acts;
- Freeze without delay funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled ... by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities...; [and]
- Prohibit their nationals or any persons and entities within their territories from making funds, financial assets or economic resources or financial or other related services available ... for the benefit of persons who commit or attempt to commit or facilitate or participate in the commission of terrorist acts, of entities owned or controlled ... by such persons and of persons and entities acting on behalf of or at the direction of such persons."[14]
- Prevent those who finance, plan, facilitate or commit terrorist acts from using their respective territories for those purposes against other States or their citizens; Ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice...."[15]

Supra-national legislation from other treaty bodies (although not strictly international law), for example in the EU Area of Freedom Security and Justice and Common Foreign and Security Policy fields also deals with intelligence cooperation.[16]

Significantly also, following the first invocation of Article 5 of the NATO treaty[17] on 12 September 2001, a range of measures was agreed by NATO countries, including enhanced intelligence sharing, blanket rights of over-flight for US and NATO aircraft for a limited period, and access to airports and ports for counter-terrorism purposes. In the view of the Venice Commission, Article 5 of the NATO treaty does not take priority over the human rights obligations under the ECHR of NATO states which are members of the Council of Europe.[18]

Finally, cooperation between international organisations and tribunals, and states or state bodies (e.g. armed forces) may be based on memoranda of understanding.

One recurring issue is the potential for conflict between a state's obligations under these bilateral or multilateral treaties and human rights norms. There has been substantial litigation, for example, concerning whether the UN terrorist blacklisting regime is compatible with human rights, especially the right to a fair trial (see section 4.3 below). In relation to bilateral agreements in particular, the risk of conflict can be mitigated by careful risk assessment before entering into these arrangements (see Chapter 6).

Recommendations:

Before entering bilateral or multilateral agreements for international intelligence cooperation, states should carefully review their compatibility with the state's international legal obligations.

All agreements for international intelligence cooperation should explicitly state that the parties' international legal obligations take priority over them.

All officers of intelligence services, whose duties involve international intelligence cooperation, should receive training in the international law implications of their work.

Intelligence services should have ready access to specialist legal advisers familiar both with these obligations and with general principles of international law.

4.3 Types of international intelligence cooperation and international law

Much international intelligence cooperation between states takes place within international law, as the previous section shows, and cooperation that violates international law may be exceptional. Nevertheless, a number of controversial practices have attracted public attention, such as rendition and other violations of international human rights law (including enforced disappearance,[19] arbitrary killing, and infringement of privacy[20]) or abuse of diplomatic facilities contrary to the Vienna Convention.[21] Consequently, more detailed consideration needs to be given to the relevant legal framework, not least to improve the accountability of the services. The purpose of this section is to discuss specific international legal standards applicable to some forms of cooperation.

As mentioned in the introduction to this chapter, under the principles of state responsibility, states may be liable when they facilitate, assist, or are complicit to breaches of human rights by their intelligence partners. Consequently, states must not knowingly "aid or assist" a wrongful act by another state,[22] nor direct and control another state in the commission of an internationally wrongful act,[23] nor coerce another state to do so.[24] Moreover, they have a duty "to cooperate to bring to an end through any lawful means any serious breach" by another state and "not to recognize as lawful a situation created by a serious breach…nor render aid or assistance in maintaining that situation."[25] In some circumstances, where in joint operations the services from two states work together so that the officials of the one are placed "at the disposal" of the other, the state of the directing service will be liable for any wrongful actions by them.[26] These principles are of general application and are used by international courts and tribunals to interpret the scope of a state's obligations,

not least under human rights law.[27] Consequently, intelligence services need to be alert to the possibility of state responsibility arising when dealing with intelligence partners who they suspect to be engaged in human rights abuses. A position of disinterested non-inquisitiveness (turning a "blind eye" to suspected abuses) is not defensible where such suspicion would be reasonable, based on credible publicly available reports documenting a partner's wrongdoing, for example from NGOs or international institutions.[28] The need for careful risk assessment before entering into bilateral arrangements is further explored in Chapter 6.

In Chapter 2, various forms of international intelligence cooperation were outlined: information sharing, covert operational cooperation, hosting facilities, providing training and advice, and providing hardware and software. It is the first three of these which are of particular concern from the perspective of international law. Nevertheless, where cooperation in training is provided to another state's services, this is also an opportunity to raise awareness concerning international legal standards, and overseers have a potential role in verifying that such training is offered to partners alongside the operational capacity building.

INFORMATION SHARING

Problematic questions arise in relation to information sharing with states that may be involved in human rights abuses, both with regard to the sending of information to partner services and in the use of information received from them. This section first discusses the question of gross human rights violations before dealing with privacy concerns, and, finally, counter-terrorism sanctions.

In some cases, outgoing information may be used to contribute to torture, unfair trials, arbitrary detention, enforced disappearance of persons, and extra-judicial killings (for example, in drone attacks). Under the rules on state responsibility (described above), states have a duty not to aid and assist in rights violations of this kind. Considerations of individual criminal liability of intelligence officers may also come into play, since the conventions against torture and enforced disappearance oblige signatory states to incorporate criminal offences covering these actions into their domestic law.[29]

Legislation governing intelligence sharing by states can help to safeguard against human rights violations. The International Commission of Jurists Eminent Jurists Panel has recommended that:

> States should establish clear policies, regulations and procedures covering the exchange of information with foreign intelligence agencies. Where such procedures exist, by way of binding instruments or understandings, they should be reviewed in light of all relevant human rights standards. In particular, information should never be provided to a foreign state where there is a credible risk that the information will cause or contribute to serious human rights violations.[30]

Recommendation:

An intelligence service should be legally obliged to use due diligence to determine that outgoing information will not be used by a partner service to assist or contribute towards violations of international human rights law, at the very least by conducting a risk assessment.

Concerning incoming information from an intelligence partner, the main issue relates to information that may have been obtained by torture or inhuman or degrading treatment in violation of international law. It is clear that a state which actively solicited information from a partner to be obtained by torture would violate international law. More common, however, is the question of a state's duty when one of its services receives *unsolicited* information from an intelligence partner in another state that may have been obtained by torture. A state receiving *unsolicited* intelligence from a partner may not be in a position to determine its source. This practical limitation does not absolve a state from due diligence in using information that it has reason to suspect is tainted in this way. For example, this concerns information coming from states where a general pattern of torture or similar abuse has been highlighted by respected NGOs or ministries of foreign affairs. The risk of complicity in torture underlines the need for an intelligence service to undertake a detailed risk assessment before passing information to, or sending interrogators or questions to a state that is known or ought to be known to engage in torture (see Chapter 6).

In its 2009 report examining potential complicity of intelligence services in torture, the UK Parliamentary Joint Committee on Human Rights summarised the implications of state responsibility for cooperation in this field. After careful review of the relevant legal arguments, the Joint Committee concluded that for the purposes on state responsibility complicity in torture "means simply one State giving assistance to another State in the commission of torture, or acquiescing in such torture, in the knowledge, including constructive knowledge, of the circumstances of the torture which is or has been taking place" (see Box 4.3).[31]

Box 4.3: State responsibility and complicity in torture: The UK Parliamentary Joint Committee on Human Rights

"[I]n our view, the following situations would all amount to complicity in torture, for which the State would be responsible, if the relevant facts were proved:

- A request to a foreign intelligence service, known for its systemic use of torture, to detain and question a terrorism suspect.
- The provision of information to such a foreign intelligence service enabling them to apprehend a terrorism suspect.
- The provision of questions to such a foreign intelligence service to be put to a detainee who has been, is being, or is likely to be tortured.
- The sending of interrogators to question a detainee who is known to have been tortured by those detaining and interrogating them.
- The presence of intelligence personnel at an interview with a detainee being held in a place where he is, or might be, being tortured.
- The systematic receipt of information known or thought likely to have been obtained from detainees subjected to torture."

Difficult questions remain about whether a state in receipt of *unsolicited* information that may have been obtained by torture should be prevented from making any use of it whatsoever. It can be argued that there is a risk that use of material of this kind, even non-judicially, creates and sustains a "market" for torture and undermines the inviolability of the international legal prohibition on torture.[32] An absolute prohibition on all use of unsolicited tainted information would be equally indefensible, however, if it prevented a state in receipt of credible intelligence of an imminent terrorist attack from taking preventative or disrupting measures (such as searching a suspect's flight luggage or evacuating members of the public in imminent danger) before checking the provenance of the information.[33] Commentators have pointed out the legal prohibitions on use of material from torture (under Article 15 of the Convention Against Torture) relate specifically to *evidence* - that is in legal proceedings - and not uses such as these.[34]

The following recommendation for a legal duty to exercise due diligence concerning incoming information takes careful account of both of the existing international legal duties and of the practical difficulties referred to.

Recommendation:

An intelligence service should be legally obliged to use due diligence to determine that incoming information has not been obtained as a result of torture, at the very least by conducting a risk assessment.

INFORMATION SHARING AND PRIVACY

Privacy is a particular area of concern in relation to information sharing. The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has noted that in the growing international effort to combat terrorism governments have endangered the protection of the right to privacy by not extending constitutional and legal safeguards over surveillance to their cooperation with third countries. The Special Rapporteur recommends that "stronger safeguards be developed to ensure that the sharing of information between governments continues to protect the privacy of individuals."[35]

Concerning outgoing information supplied to partner services, it is important to understand that human rights norms apply not only to the collection of personal information but also to decisions over sharing and disclosing it. Within Council of Europe states, disclosure to other authorities of information obtained by surveillance or held in security files is treated as a distinct act of interference with the right of private life (Article 8 ECHR) that requires specific legal authority.[36] The legislation must, therefore, not only explicitly state that such information may be shared with foreign services but also the circumstances when this is permissible, which according to Convention standards must meet the legitimate aims for interference and be necessary and proportionate.[37]

The processing, analysis, and communication of incoming material by a receiving state is clearly within its jurisdiction and is governed by a state's human rights obligations

(as well as national law).[38] This brings use by a receiving state of information shared by foreign partners within the scope the privacy norms under human rights law. Use of any information collected by the state extra-territorially will also be within its jurisdiction. According to the Venice Commission, "[a] particular issue, bearing in mind the close cooperation which allegedly exists between certain Western signals intelligence agencies, is the risk of circumvention of stronger domestic surveillance procedures."[39] There is a danger that an intelligence service could seek to avoid or circumvent limitations in domestic law on surveillance by actively requesting a foreign partner to conduct surveillance on its nationals or residents and to share it. This is best addressed by a specific legal prohibition on practices involving circumvention of domestic legal controls, as we propose in Chapter 5.[40]

Moreover, as noted in Chapter 2, "information sharing" also covers access to bulk strategic surveillance conducted under shared arrangements.[41] Here, questions of the location of interference are increasingly irrelevant, due both to the complex nature of modern communications technology and the means that states use to collect and access this data.

This also poses a challenge for states whose law confers additional privacy protection on nationals or persons resident within the territory, since to give effect to these protections would require an intelligence service to be able to identify an internet user's nationality. The objective of such provisions is laudable.[42] However, even if it could be successfully implemented, it is doubtful if this approach complies with international law, since it involves discrimination in the enjoyment of the human rights protected by the state. This is contrary both to the ICCPR (Articles 2 and 26) and regional human rights treaties such as the ECHR (Article 14), whereas human rights are to be enjoyed by "everyone" regardless of nationality. Against the background of the Snowden revelations, the UN Human Rights Committee stated in 2014 that the United States should:

> Take all necessary measures to ensure that its surveillance activities, both within and outside the United States, conform to its obligations under the Covenant, including article 17; in particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance.[43]

International bodies have treated the use of search terms to search bulk data as equating to more traditional forms of surveillance in terms of the interference with the right of privacy.[44] It is important, therefore, that searches of bulk data are adequately authorised and limited by domestic law. Practice of this kind seems to be the exception rather than the norm; relatively few countries have legislation on strategic surveillance and the jurisprudence of international courts is sparse. This is an area where, following the Snowden revelations, the implications of human rights principles are in the process of being clarified. A pending case at the European Court of Human Rights concerning the activities of the UK signals intelligence service GCHQ is likely to provide further guidance on how specific such laws need to be in order to meet international standards.[45] A recent report from the Council of Europe's Venice Commission has stressed the need for parliamentary supervision in "deciding the general rules regarding who, and under

what circumstances, signals intelligence can be exchanged with other signals intelligence organisations" and for follow-up oversight by an independent expert administrative body of decisions to transfer personal data collected to foreign services.[46]

INFORMATION SHARING AND COUNTER-TERRORISM SANCTIONS[47]

As noted above, one specific method for international cooperation that has grown in importance in the last 15 years is the use of controls to prevent the flow of financing to terrorist groups. The origins of anti-terrorism financial measures lie in Resolution 1267 passed in 1999 by the UN Security Council following the bombing of the United States' embassies in Nairobi and Dar es Salaam, which provided for the freezing of funds and other financial resources derived or generated from property owned or controlled by the Taliban, or by any undertaking owned or controlled by them.[48] A sanctions Committee was established to oversee implementation of these measures, known as the 1267 Committee.[49] This Committee maintains what is now known as the "Al-Qaeda List" (or "Consolidated List") of individuals and entities associated with Al-Qaeda, Osama bin Laden, and/or the Taliban, against which all states must impose asset-freezes, travel bans, and arms embargos.[50]

The current procedure requires Member States to provide a detailed statement of case in support of a proposed listing of an individual containing: specific finding demonstrating the association or activities alleged; the nature of the supporting evidence (e.g. intelligence, law enforcement information, judicial determination, media, or admissions by the subject); and supporting evidence or documents that can be supplied.[51] States shall identify those parts of the statement of case that may be publicly released. The Committee makes a narrative summary of the reasons for listing available on its website. The Committee acts by consensus and usually meets in private.

The Committee also considers petitions for removal from the Consolidated List of those who no longer meet the criteria ("delisting"). The Security Council created the Office of the Ombudsperson by Resolution 1904 (2009) to whom application for delisting can be addressed. The Office of the Ombudsperson provides a route for limited disclosure of information to the person affected (subject to issues of confidentiality) and, therefore, the opportunity to respond to that case and provide information that is reflected in the Ombudsperson's report.[52] The Ombudsperson's recommendations are not binding on the Committee.

In order to give effect to these UN resolutions within the European Union, the Council adopted Regulation (EC) No 881/2002 ordering the freezing of the funds and other economic resources of the persons and entities whose names appear on a list annexed to that Regulation. A number of EU states rely on the Regulation as sufficient legal basis for domestic financial measures, whereas others (like the UK) have passed specific national legislation.

The listing and delisting processes under the sanctions regimes have been criticised for denying or restricting the human rights of those listed to a fair trial, family and private life,

and the enjoyment of property and have been the subject of extensive litigation before international and domestic courts.[53]

COVERT OPERATIONAL COOPERATION

There are different ways in which international legal responsibility or liability may be engaged when intelligence services cooperate in operations with foreign counterparts. States may engage in forms of intelligence cooperation that directly violate international law, for example, where the agents of one state conduct rendition in another state with its assistance or permission,[54] where it engages in extra-judicial killings (for example by drone attacks) of terrorist suspects (or, unintentionally, of non-suspects),[55] or conducts joint surveillance in violation of international human rights law.

A state that operates facilities or conducts operations in the territory of another state may be liable if these actions are deemed to fall within its "jurisdiction" for the purposes of a relevant human rights treaty obligation, such as Article 2 of the ICCPR[56] or Article 1 of the European Convention on Human Rights.[57] "Jurisdiction" primarily refers to acts in a state's own territory. However, exceptionally, extra-territorial liability may arise where a state conducting operations has effective control over the person whose rights are violated or over the geographical space in which violations occur.

Box 4.4: Liability for extraterritorial intelligence activities under the ECHR

Under the European Convention on Human Rights "whenever the State, through its agents operating outside its territory, exercises control and authority over an individual, and thus its jurisdiction, the State is under an obligation to secure the rights under the Convention to that individual."[58] The obligation can arise in three distinct ways:[59]

- The acts of diplomatic and consular agents, who are present on foreign territory in accordance with provisions of international law […] when these agents exert authority and control over others.
- When, through the consent, invitation or acquiescence of the Government of that territory, it exercises all or some of the public powers normally to be exercised by that government.
- The use of force by a State's agents operating outside its territory may bring the individual thereby brought under the control of the State's authorities into the State's Article 1 ECHR jurisdiction.[60]

Some examples show how this principle can cover actions of state officials falling within international intelligence cooperation. It applies, for example, in the case of suspects within an army base operated by forces of the state in a partner state,[61] for actions in the embassy of the state,[62] or where a detained person is held on a military aeroplane[63] or a ship of the state on the high seas.[64]

It is important to bear in mind that, even if the state on whose territory intelligence operations occur consents to the activities in question, this cannot confer immunity

for some breaches of international human rights law. The consent may, however, also implicate the state on whose territory the act takes place. States that permit the action of another state in their territory that violates peremptory norms or international human rights obligations may also be responsible in international law.[65] Examples may include hosting facilities of another state in which violations occur (such as so called black sites),[66] permitting officials from another state to abduct a suspect from the consenting state's territory[67] or allowing intelligence operatives, who are in the course of committing violations, to land and refuel, over-fly, or pass through territory.[68] In particular, states can be liable indirectly for complicity and providing assistance for violation of the prohibitions on torture,[69] arbitrary detention,[70] and enforced disappearance.[71]

(JOINT) INTERROGATION BY SERVICES

The use of torture is absolutely prohibited as a peremptory norm of international law, and no derogation is permitted from it.[72] There are no circumstances in which it can ever be appropriate for an intelligence service or intelligence officials to resort to it. As regards cooperation with intelligence partners, all other obligations of the state, including those under treaties, status of forces agreements, or the non-treaty arrangements cannot override the prohibition on torture and have to be interpreted consistently with it.

In addition, nearly all states are bound by the ICCPR (Art. 7) which prohibits torture,[73] and more than three-quarters of all states are parties to the more detailed UN Convention Against Torture.[74] The Convention potentially impacts intelligence cooperation in several ways (illustrated in Box 4.2). Intelligence services cannot engage in any form of "torture by proxy" or "outsourcing" of torture: directing or controlling torture through an intelligence partner or a contractor is clearly prohibited in the same way as if torture were conducted by the intelligence service itself.[75] Equally, providing aid or assistance (which may include sharing information) to a partner state in engaging in torture is clearly contrary to international law. Falling short of direct responsibility there are several ways in which the possibility of torture may taint intelligence cooperation and which raise the risk that intelligence services or officials may be complicit in torture practised by other states[76] (illustrated in Box 4.3).

HOSTING FACILITIES

The existence of premises or forces permitted by the host state raises questions of the host state's responsibility for the actions of the operating state's officials that take place there. Host states may be precluded by their consent from taking international legal action against the operating state,[77] but this does not affect any liability that they have for aiding or assisting any wrongful acts.[78] Moreover, there is a duty under the International Law Commission (ILC) articles on state responsibility to cooperate to bring a serious breach to an end and not to recognise the situation as lawful.[79]

Box 4.5 illustrates the responsibilities of a cooperating state in international law for various types of joint operations and other forms of international intelligence cooperation in its own territory. The box gives a number of examples but these are not exhaustive.

Box 4.5: Examples of joint operations and their implications in international law

Activity	Liability of Cooperating State
Acting with foreign service to detain a suspect and send him/her to another state for harsh interrogation.	• A state is prevented from expelling, returning ("refouler") or extraditing a person to another state "where there are substantial grounds for believing that he would be in danger of being subjected to torture." (CAT Art. 3.1; ICCPR Art. 7; ECHR, Art. 3)[80]
Acting with a foreign service to conduct surveillance, including through hosting surveillance facilities.	• Failure to "secure" protection of rights to everyone within its jurisdiction including the right of respect for private life (ICCPR Art. 17; ECHR Art 8).[81]
Allowing a foreign service to abduct a suspect in its territory.	• Breach of the state's duty to secure effective protection of human rights to everyone within the state's jurisdiction (e.g. ICCPR, Art. 2; ECHR, Art. 1). • Cooperating state may be liable for breach of prohibition on arbitrary detention (ICCPR, Art. 9; ECHR, Art. 5)[82].
Allowing a foreign service to detain, question and torture suspects in its territory	• Hosting state may itself be in breach of the prohibition on torture (e.g. Art 3 ECHR) by facilitating or conniving in torture.[83] • CAT, Art 2 requires a state party to take effective legislative, administrative, judicial or other measures to prevent acts of torture in any territory under its jurisdiction.[84] A state has a positive obligation to investigate under CAT, Arts 12 and 13 • Aiding or assisting torture is also prohibited under ICCPR Art. 7.

Recommendation:

A state that hosts intelligence facilities of a partner state or permits a partner intelligence service to operate in its territory should ensure that the arrangements for doing so allow it to fully discharge its own obligations under international human rights law.

Human rights law does not allow a host state to turn a blind eye to the actions of intelligence partners in its territory because the duty to secure human rights within its jurisdiction entails a number of specific positive obligations. As mentioned above, there is a positive obligation to conduct a prompt and impartial investigation wherever there is reasonable ground to believe that torture has occurred in its jurisdiction.[85] A comparable duty applies under the Convention on Enforced Disappearance.[86] Moreover, as explained in Chapter 8, where a state ought to be aware of the risk of torture or of arbitrary detention at the hands of its partners operating in its territory, it will be in breach itself if it fails to take steps to prevent it.[87] Consideration should therefore be given to including in agreements governing cooperation activities practical powers to enable the hosting state to fulfil its international legal responsibilities, for example, to inspect facilities, a duty for the hosted partner agency to cooperate with human rights investigations, and the option of terminating the arrangement for human rights abuses.

4.4. Cooperating with legal proceedings and international investigations

Generally speaking, a state's duties in international law to cooperate with international legal proceedings and investigations follow from its specific multi-lateral treaty commitments. For example, under the Rules of the European Court of Human Rights, the Court may request evidence from a member state, and the Court has power to conduct investigations, including visits to the territory of a member state, with which the state must cooperate.[88] Articles 12 and 13 of the Convention Against Torture impose a direct positive obligation on states to investigate participation in torture and complicity in torture in their territory or under their jurisdiction.[89]

Where a state has accepted the competence of the relevant monitoring body to hear individual petitions (for example, to the UN Committee Against Torture or to the Human Rights Committee), the process can result in detailed examination of the degree of its involvement in human rights breaches arising from international intelligence cooperation.[90] Complaints of this kind may also indirectly examine actions of intelligence partners that have not accepted the right of individual petition. The systems of periodic reporting by human rights bodies have likewise provided a degree of scrutiny of some international intelligence cooperation activities.

Some international bodies within Europe (especially the Parliamentary Assembly of the Council of Europe and the European Parliament) have established inquiries into intelligence activities involving international intelligence cooperation. Examples are the EP inquiry on *The Echelon interception system*;[91] the EP inquiry on *The alleged use of European countries by the CIA for the transportation and illegal detention of prisoners*;[92] the PACE inquiry on *Secret detentions and illegal transfers of detainees involving Council of Europe member states*;[93] and the recent inquiries into mass surveillance.[94]

However, inquiries of this kind are hampered by limited legal powers with the result that the pressure that can be brought to bear on states to cooperate is largely political in

nature. In the absence of cooperation, the effectiveness of any investigation is dependent on whistle-blowers and the work of NGOs and investigative journalists. The EP can establish a committee of inquiry to examine alleged contraventions of European Community (EC) law or "mal-administration" in the application of this law.[95] Since the Lisbon Treaty, some questions of international intelligence cooperation will fall within the field of Community law[96] (and hence can be subject to a committee of inquiry), but states are permitted to withhold information for reasons of secrecy, public and/or national security.[97]

Within the Parliamentary Assembly of the Council of Europe, the Assembly's rules of procedure permit its committees to examine any matter within their terms of reference; in the case of the Committee on Legal Affairs and Human Rights terms extend to "all legal and human rights matters which fall within the competence of the Council of Europe."[98] These committees have almost no legal powers to assist them in their work. The Secretary-General of the Council of Europe may, under Article 52 of the European Convention on Human Rights, request "any High Contracting party […to] furnish an explanation of the manner in which its internal law ensures the effective implementation of any of the provisions of this Convention." In 2005, the Secretary-General used these powers to request information from member states on how their internal law ensured the effective implementation of the ECHR on four issues:

1. adequate controls over acts by foreign agents in their jurisdiction;
2. adequate safeguards to prevent, as regards any person in their jurisdiction, unacknowledged deprivation of liberty, including transport, with or without the involvement of foreign agents;
3. adequate responses (including effective investigations) to any alleged infringements of ECHR rights, notably in the context of deprivation of liberty, resulting from conduct of foreign agents; and
4. whether since 1 January 2002 any public official has been involved, by action or omission, in such deprivation of liberty or transport of detainees; whether any official investigation is under way or has been completed.[99]

The powers to conduct investigations complement the judicial processes of the Council of Europe, and by cooperating in investigations in this way states can provide reassurance that their international intelligence cooperation activities are compatible with their international legal obligations.

Endnotes

1. Art. 4, Articles on Responsibility of States for Internationally Wrongful Acts (2001): see General Assembly Resolution 56/83, *Responsibility of States for internationally wrongful acts*, A/RES/56/83 (28 January 2002) and ILC, *Report of the ILC; ILC Yearbook 2001*, Vol II(2), 26-143.
2. UN Committee Against Torture (CAT), *UN Committee against Torture: Conclusions and Recommendations*, United States of America, 25 July 2006, CAT/C/USA/CO/2, para. 17.
3. Art. 7, Articles on Responsibility of States for Internationally Wrongful Acts.
4. Art. 8, Articles on Responsibility of States for Internationally Wrongful Acts.
5. See Article 2.1 of the 1969 Vienna Convention on the Law of Treaties.
6. Reference may also be made to: 'political agreements', 'provisional understanding', 'exchanges of notes', 'administrative agreements', 'terms of reference' or 'declarations': see Martin Scheinin and Mathias Vermeulen, "Human Rights Law and State Responsibility" in *International intelligence cooperation and accountability*, ed., Hans Born, Ian Leigh and Aidan Wills, (London: Routledge, 2011), 256.
7. "NSA and Israeli intelligence: memorandum of understanding – full document," *The Guardian*, 11 September 2013, The memorandum was leaked by Edward Snowden and its contents have not been confirmed by the parties.
8. For example the USAF base at Menwith Hill in the UK. "The base at Menwith Hill is a signals intelligence field site that supports U.S., U.K. and N.A.T.O communications and communications research interests". Per Lord Hope of Craighead in *Holland v. Lampen-Wolfe* (2000) UKHL 40, discussing the question of state immunity in relation to statements made by a member of personnel stationed there.
9. Non-treaty arrangements between states can also operate multi-laterally, for example cooperation within the Club of Berne (see Chapter 2).
10. See Section 4.3 below.
11. See further Simon Chesterman, "Intelligence Cooperation in International Operations: peacekeeping, weapons inspections, and the apprehension and prosecution of war criminals," in *International intelligence cooperation and accountability*.
12. UN Security Council resolution 1371, *Threats to international peace and security caused by terrorist acts*, 28 September 2001, S/RES/1373 (2001).
13. S/RES/1373 (2001), paras. 3 (a) and (b).
14. S/RES/1373 (2001), para.1 (a)-(d). The use of international financial measures targeted at individuals and companies is not, however, confined to anti-terrorism. Sanctions of this kind are a feature, in particular, of measures against non-proliferation and other violations of international law.
15. S/RES/1373 (2001), para.2 (d).
16. European Parliament, Policy Department C: Citizens' Rights and Constitutional Affairs, *Parliamentary oversight of civilian security and intelligence agencies in the European Union*, (Brussels, 2011), 407-8.
17. Article 5 of the NATO Treaty states that an armed attack against one Ally shall be considered an attack against them all. In response to an invocation of Article 5, each Ally determines, in consultation with other Allies, how it can best contribute to any action deemed necessary to restore and maintain the security of the North Atlantic area, including by the use of armed force.
18. Council of Europe, European Commission for Democracy through Law (Venice Commission), *Opinion on the international legal obligations of Council of Europe member States in respect of secret detention facilities and inter-State transport of prisoners*, 17 March 2006, Opinion No. 363/2005. paras. 111-115.
19. Enforced disappearance is defined, under Article 2 of the International Convention for the Protection of All Persons from Enforced Disappearance, as: "the arrest, detention, abduction or any other form of deprivation of liberty by agents of the State or by persons or groups of persons acting with the authorization, support or acquiescence of the State, followed by a refusal to acknowledge the deprivation of liberty or by concealment of the fate or whereabouts of the disappeared person, which place such a person outside the protection of the law."
20. Protected under Art. 17 ICCPR; Art. 8 ECHR.
21. Venice Commission, Opinion No. 363/2005, paras. 111-115.
22. International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts* (ARSIWA), 2001, Article 16.
23. Article 17 ARSIWA.
24. Article 18 ARSIWA.
25. Article 41 ARSIWA.
26. Article 6 ARSIWA.
27. For more detailed discussion of their application to international intelligence cooperation see: Martin

Scheinin and Mathias Vermeulen, "Human Rights Law and State Responsibility" in *International intelligence cooperation and accountability*.

28. See for example, *Al Nashiri v. Poland*, no. 28761/11, 24 July 2014 and *Husayn (Abu Zubaydah) v. Poland*, no. 7511/13, 24 July 2014, discussed in Chapter 8.
29. Convention Against Torture, Art. 4 (referring specifically also to participation and complicity in torture); International Convention for the Protection of All Persons from Enforced Disappearance, Art. 4.
30. International Commission of Jurists Eminent Jurists Panel, *Assessing Damage, Urging Action*, (Geneva, 2009), 90.
31. UK, Joint Committee on Human Rights, *Allegations of UK Complicity in Torture, 23rd Report* (2008-2009), paras. 29-35.
32. See Martin Scheinin and Mathias Vermeulen, "Human Rights Law and State Responsibility" in *International intelligence cooperation and accountability*; UN Special Rapporteur for Promotion and protection of human rights and fundamental freedoms while countering terrorism, *The Role of Intelligence Agencies and Their Oversight in the Fight against Terrorism*, A/HRC/10/3, 4 February 2009, section 55.
33. See discussion of a Canadian Ministerial Direction to CSIS on "Information Sharing with Foreign Agencies" of 14 May 2009 in Craig Forcese, "Vic Toews, Kant and Mill: Torture Again."
34. S. Borelli, "Rendition, torture and intelligence cooperation," in *International intelligence cooperation and accountability*, 106. And see in particular *A v. SSHD* (no. 2) [2005] UKHL 71, at [47]-[48] (Lord Bingham); [67]-[78], (Lord Nicholls); [92]-[93] (Lord Hoffmann); [149], (Lord Carswell); and [161]-[162] and [166]-[171], (Lord Brown).
35. UN Special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, *4th annual report*, 23 September 2014, A/69/39, para. 65.
36. See decisions of the European Court of Human Rights in Rotaru v. Romania, no. 28341/95, ECtHR 2000, para. 46; *Weber and Saravia v. Germany*, no. 54394/00, ECtHR 2006, para.79.
37. See the decision of the (UK) Investigatory Powers Tribunal applying this approach to the sharing of information by GCHQ: *Liberty and others v. The Secretary of State for Foreign and Commonwealth Affairs and others*, no. IPT/13/77/CH; 13/92/CH; 13/194/C and 13/204/CH, [2015] UKIPTrib 13_77–H.
38. In *Weber and Saravia v. Germany* the European Court of Human Rights noted that "Signals emitted from foreign countries are monitored by interception sites situated on German soil and the data collected are used in Germany," para. 88.
39. Venice Commission, *Update of the 2007 Report on Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies*, CDL-AD (2015) 06, para. 78.
40. Venice Commission, *Update of the 2007 Report* para. 78. This will not, however, in itself prevent passive receipt of such information among states with closely integrated signals intelligence capability, such as the UKUSA partners.
41. On this topic see the important study by the Venice Commission, *Update of the 2007 Report*.
42. They may be intended to act as a safeguard against the circumvention of stricter controls over surveillance of internal communications.
43. Human Rights Committee, *Concluding Observation on the Fourth Periodic Report by the United States of America*, CCPR/C/USA/CO/4, para 22.
44. *Weber and Saravia v. Germany*, no. 54394/00, ECtHR 2006; Venice Commission, *Update of the 2007 Report*.
45. *Big Brother Watch and Others v. the United Kingdom*, no. 58170/13, 7 January 2014 in which the applicants claim that probable surveillance by the United Kingdom security services in receipt of foreign intercept material relating to their electronic communications was not "in accordance with the law" under Article 8 ECHR. They argue that there was a lack of basis in domestic law for the receipt of information from foreign intelligence agencies and of legislative control and lack of safeguards over the circumstances in which the UK intelligence services can request foreign intelligence agencies to intercept communications and share access to the data obtained, and the extent to which the UK can use, analyse, disseminate, store, and destroy data solicited or received in this way. The same question was addressed in the UK by the Investigatory Powers Tribunal which found that the scheme had indeed been in violation of Article 8 but that this defect had been cured for the future by the disclosure (during the proceedings in question) of previously secret internal guidance: *Liberty and others v. The Secretary of State for Foreign and Commonwealth Affairs and others*, no. IPT/13/77/CH; 13/92/CH;

13/194/C and 13/204/CH, [2015] UKIP Trib 13_77–H at 153-154. The (UK) Independent Reviewer of Terrorism Legislation has recommended a series of detailed legislative reforms to govern the collection of bulk communications: Independent Reviewer of Terrorism Legislation, *A Question of Trust: Report of the Investigatory Powers Review*, 2015.

46. Venice Commission, *Update of the 2007 Report*, para. 25.
47. Ian Cameron, "Blacklisting and Financial Sanctions against Suspected Terrorists" in *International intelligence cooperation and accountability*.
48. UN Security Council resolution 1267, 15 October 1999, S/RES/1267, para 4(b).
49. S/RES/1267 concerning Al-Qaida and the Taliban and Associated Individuals and Entities'Al Quaida and the Taliban.
50. For the current list see: http://www.un.org/sc/committees/1267/AQList.htm
51. UN Security Council Resolution 1822, *Threats to international peace and security caused by terrorist acts*, 30 June 2008, S/RES/1822. See also: Security Council Committee Established Pursuant to Resolution 1267 (1999) concerning Al-Qaida and the Taliban and Associated Individuals and Entities, Guidelines of the Committee for the Conduct of its Work, 9 December 2008.
52. In relation to other UN sanctions regimes Resolution 1730 (2006) establishes a 'Focal Point' in the UN Secretariat is established as a central point for de-listing requests from listed individuals or entities. These requests are forwarded to the designating state(s) and to the state(s) of nationality and residence for their information and possible comments.
53. For example: *Joined Cases C-584/10, C-593/10 & C-595/10, Kadi v. European Commission* (European Court of Justice 18 July 2013) (Kadi II); *In Her Majesty's Treasury (Respondent) v. Mohammed Jabar Ahmed and others (FC) (Appellants); Her Majesty's Treasury (Respondent) v. Mohammed al-Ghabra (FC) (Appellant); R (on the application of Hani El Sayed Sabaei Youssef) (Respondent) v. Her Majesty's Treasury (Appellant)* [2010] UKSC 2.
54. Where there is no permission the action will constitute a violation of sovereignty: See *The SS "Lotus", 1927, Permanent Court of International Justice, Series A, no. 10*, at 18-19; see also Security Council Resolution 138 (1960) in relation to the abduction of Adolf Eichmann.
55. UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, *The use of remotely powered aircraft in counter-terrorism operations*, UN Doc. A/68/389 (18 September 2013); see Chapter 8 for litigation that has been brought concerning intelligence supplied that has allegedly assisted in drone attacks.
56. Human Rights Committee, General Comment No. 31, *The Nature of the General Legal Obligations Imposed on State Parties to the Covenant*, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (2004). para. 10; Human Rights Committee, *Lopez Burgos v. Uruguay*, Communication, no. 52/79 (A/36/40) at 176 (1981), paras. 12.1-12.3.
57. See *Al-Saadoon and Mufdhi v UK*, no. 61498/08, ECtHR, 2 March 2010 (finding that the UK breached Art. 3 ECHR by transferring applicants from military custody to Iraqi authorities to face trial where they were liable to the death penalty).
58. *Hirsi Jamaa v. Italy* ECtHR, no. 27765/09, ECtHR (Grand Chamber), 23 February 2012, para. 74.
59. See generally *Al-Skeini and Others v UK* no. 55721/07, ECtHR (Grand Chamber), 7 July 2011, paras. 134-136.
60. Note that in this instance: "[t]he Court does not consider that jurisdiction in the above cases arose solely from the control exercised by the Contracting State over the buildings, aircraft or ship in which the individuals were held. What is decisive in such cases is the exercise of physical power and control over the person in question." (para. 136)
61. For example, the clandestine detention and interrogation facilities operated by the United States Central Intelligence Agency in several countries.
62. *M v. Denmark*, no. 17392/90, E Comm HR, 14 October 1992 (admissibility), arising from the invitation by the Danish ambassador to East German police to enter the Danish embassy to arrest the applicant.
63. *Ocalan v. Turkey*, no. 46221/99, Grand Chamber, 12 May 2005, 41 EHRR 45; *Illich Sanchez Ramirez v. France*, no. 28780/95, E CommHR, 24 June 1996 (admissibility), terrorist suspect under jurisdiction

of France when handed over in Sudan to be put on a French military aircraft, but no admissible claim from the facts alleged for breach of Arts. 3 or 5.

64. *Hirsi Jamaa v. Italy* ECHR, no. 27765/09, ECtHR (Grand Chamber), 23 February 2012, violation arising from interception of immigrants, transfer onto Italian military vessels and return to Libya pursuant to bi-lateral agreement between Italy and Libya.

65. PACE, Committee on Legal Affairs and Human Rights (Rapporteur: D. Marty), *Secret detentions and illegal transfers of detainees involving Council of Europe member states: Second report*, 11 June 2007, doc. 11302/rev; European Parliament, Temporary Committee on the alleged use of European countries by the CIA for the transport and illegal detention of prisoners (Rapporteur: G.C. Fava), *Report on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners*, 30 January 2007, doc. A6-0020/2007; see also *Working Document No. 7 on 'extraordinary renditions'*, 16 November 2006, PE-380-593.

66. According to the PACE report, secret detention facilities in Poland and Romania were created as part of the CIA High-Value Detainees Programme, on the basis of "operating agreements" concluded between the CIA and the governments of Poland and Romania. Under those agreements, "Poland and Romania agreed to provide the premises in which these facilities were established, the highest degrees of physical security and secrecy, and steadfast guarantees of non-interference," PACE, Committee on Legal Affairs and Human Rights (Rapporteur: D. Marty), para.117. See further *Al Nashiri v. Poland*, no. 28761/11, 24 July 2014 (discussed in Box 8.8); *Husayn (Abu Zubaydah) v. Poland*, no. 7511/13, 24 July 2014.

67. See the Abu Omar case, discussed in Chapter 8.

68. Venice Commission, *Opinion on the international legal obligations of Council of Europe member States in respect of secret detention facilities and inter-State transport of prisoners* (2006), no. 363/2005, paras 86-104, 137-153. And see Irish Human Rights Commission, *Extraordinary Rendition: A Review of Ireland's Human Rights Obligations*, first published in December 2007.

69. Box 4.3.

70. In its opinion No. 11/2007,(A/HRC/7/4/Add.1) the UN Working Group on Arbitrary Detention, concurring declared the Government of Afghanistan responsible for the arbitrary detention of an individual who was being detained at Bagram Airbase, under the control of the United States of America, but on Afghan soil with the knowledge of Afghan authorities. See also: *Joint Study on Global Practices in Relation to Secret Detention in the Context of Countering Terrorism*, UN General Assembly, Human Rights Council, A/HRC/13/42, 19 February 2010.

71. European Court of Human Rights: *El-Masri v. FYR Macedonia*, no. 39630/09, 13 December 2012 (see Box 8.7).

72. *Prosecutor v. Furundzija*, no. IT-95-17/1-T, Judgment para 153 (ICTY Trial Chamber 10 December 1998); CCPR/C/21/Rev.1/Add.6 (1994), Human Rights Committee, General Comment 24, Issues relating to reservations made upon ratification or accession to the Covenant or the Optional Protocols thereto, or in relation to declarations under article 41 of the Covenant, para. 10.

73. ICCPR article 7 also applies to inhuman, cruel or degrading treatment or punishment, including in the context of extradition or transfer of a person to another state under the risk of prohibited treatment. See, CCPR/C/88/D/1416/2005, *Mohammed Alzery v. Sweden*, 10 November 2006, CCPR/C/80/D/1051/2002 (2004), *Mansour Ahani v. Canada*, 29 March 2004, para.10.10, CCPR/C/76/D/900/1999, *C. v. Australia*, 28 October 2002, paras. 8.4.-8.5. For regional human rights prohibitions on torture see: African Charter on Human and People's Rights, Art. 5; Arab Charter on Human Rights, Art. 8; European Convention on Human Rights, Art. 3.

74. Article 1 of the Convention defines torture as: "any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person for such purposes as obtaining from him or a third person information or a confession, punishing him for an act he or a third person has committed or is suspected of having committed, or intimidating or coercing him or a third person, or for any reason based on discrimination of any kind, when such pain or suffering is inflicted by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity. It does not include pain or suffering arising only from, inherent in or incidental to lawful sanctions."
Article 2 requires States to take effective legislative, administrative, judicial or other measures to prevent acts of torture in any territory under its jurisdiction. Article 4 requires each State Party to ensure that all acts of torture are offences

under its criminal law.

75. The definition of torture in article 1 of CAT includes acts "inflicted by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity."
76. States are required by the Article 4 of CAT to ensure that any act by any person which constitutes complicity or participation in torture is an offence under criminal law.
77. ILC Article 20.
78. ILC Article 16: "A State which aids or assists another State in the commission of an internationally wrongful act by the latter is internationally responsible for doing so if: (a) that State does so with knowledge of the circumstances of the internationally wrongful act; and (b) the act would be internationally wrongful if committed by that State."
79. ILC Article 41. A 'serious breach' means a breach of a peremptory norm of international law that involves a "gross or systematic failure" to meet the obligation that such a norm entails. See also Martin Scheinin and Mathias Vermeulen, "Human Rights Law and State Responsibility" in *International intelligence cooperation and accountability*.
80. In determining whether there are such grounds, the competent authorities shall take into account "all relevant considerations including the existence in the State concerned of a consistent pattern of gross, flagrant or mass violations of human rights." (art. 3.2); See CCPR/C/88/D/1416/2005, *Mohammed Alzery v. Sweden*, 10 November 2006, CCPR/C/80/D/1051/2002; European Court of Human Rights: *El-Masri v. FYR Macedonia* no. 39630/09, 13 December 2012, para. 212 (see Box 8.7); *Al Nashiri v. Poland* No. 28761/11, 24 July 2014, para. 454 (discussed in Box 8.8).
81. See generally: The right to privacy in the digital age, *Report of the Office of the United Nations High Commissioner for Human Rights*; European Parliament, LIBE, *Report on the US NSA surveillance programme, surveillance bodies in various*. Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)) PACE, Committee on Legal Affairs and Human Rights, *Mass surveillance*, Rapporteur: Mr Pieter Omtzigt (April 2015).
82. This was the finding in *Al Nashiri v. Poland* No. 28761/11, 24 July 2014, para. 455 (discussed in Box 8.8).
83. Ibid., para. 517.

See Venice Commission, *Opinion No. 363/2005, on the international legal obligations of Council of Europe member States in respect of secret detention facilities and inter-State transport of prisoners* (2006)

84. See General Comment no. 20: concerning prohibition of torture and cruel treatment or punishment, 10 March 1992.
85. CAT, Arts 12 and 13. The European Court of Human Rights has interpreted Art. 3 ECHR to impose a similar procedural duty on a state to carry out an effective investigation.
86. Article 12.
87. See discussion of *Al Nashiri v. Poland* No. 28761/11, 24 July 2014, para. 455, with regard to Art. 3 ECHR (Box 8.8)
88. See European Court of Human Rights, Rules of Court 2013.
89. Article 12 provides that each State Party shall ensure that its competent authorities proceed to a prompt and impartial investigation, wherever there is reasonable ground to believe that an act of torture has been committed in any territory under its jurisdiction. Article 16 CAT imposes the same obligations with respect to investigation of allegations of inhuman or degrading treatment.
90. See, in particular, Committee Against Torture, *Agiza v. Sweden* (Comm. 233/2003), Views of 20 May 2005, CAT/C/34/D/233/2003; Human Rights Committee, *Alzery v. Sweden* (Comm. 1416/2005), Views of 25 October 2006, CCPR/C/88/D/1416/2005. Cf. *Alzery v. Sweden*, no. 10786/04, ECtHR, decision on admissibility of 26 October 2004.
91. *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)*, A5-0264/2001 (Brussels/Strasbourg: 11 July 2001); European Parliament, *Resolution setting up a temporary committee on the Echelon interception system*, B5-0593/2000/rev, 5 July 2000.
92. See European Parliament, *Transportation and Illegal Detention of Prisoners; Resolution on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners*, INI/2006/2200, 14 February 2007.
93. Parliamentary Assembly of the Council of Europe, Doc. 11302 rev. 11 June 2007, Secret detentions and illegal transfers of detainees involving Council of Europe member states: second report, Report Committee on Legal Affairs and Human

Rights, Rapporteur: Mr Dick MARTY, Switzerland; Resolution 1562 *Assembly Text adopted by the Assembly* on 27 June 2007 (23rd Sitting).

94. The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights; European Parliament, LIBE, *Report on the US NSA surveillance programme, surveillance bodies in various*. Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)); PACE, Committee on Legal Affairs and Human Rights (Rapporteur: Mr Pieter Omtzigt), *Mass surveillance*, April 2015.
95. European Parliament, *Rules of Procedure for the 7th parliamentary term*, (Brussels/Strasbourg, 2010), Rule 185; European Parliament, *Report on the existence of a global system for the interception of private and commercial communications* (ECHELON interception system), A5-0264/2001, (Brussels/Strasbourg, 11 July 2001), 22-23.
96. This was not the case at the time of the Echelon and TDIP inquiries, which were established instead by resolutions of the EP as temporary committees of the EP. For the TDIP inquiry see European Parliament, *Decision setting up a temporary committee on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners*, 18 January 2006; For the Echelon inquiry: European Parliament, *Resolution setting up a temporary committee on the Echelon interception system*, B5-0593/2000/rev, 5 July 2000.
97. Decision of the European Parliament, the Council and the Commission on the detailed provisions governing the exercise the European Parliament's right of inquiry, 19 April 1995, Article 3(4).
98. PACE, *Rules of Procedure* (Strasbourg, January 2008), 44.1; PACE, *Terms of Reference of Assembly Committees*, (Strasbourg: January 2008), Section II: Committee on Legal Affairs and Human Rights (AS/Jur), 1, and 2 (v).
99. Council of Europe/Secretary General, *Report by the Secretary-General on the use of his powers under Article 52 of the European Convention on Human Rights, in the light of reports suggesting that individuals, notably persons suspected of involvement in acts of terrorism, may have been arrested and detained, or transported while deprived of their liberty, by or at the instigation of foreign agencies*, SG/Inf (2006) 5, 28 February 2006.

5

Domestic Legal Framework for International Intelligence Cooperation

5.1 Introduction

Whereas Chapter 4 deals with the treatment of international intelligence cooperation in international law and Chapter 8 considers the role of national and international courts, the focus of this chapter is on the treatment of international intelligence cooperation in domestic law and policy. The need to regulate international cooperation through domestic law is first discussed, followed by the different approaches that countries adopt in domestic security and intelligence legislation. Special attention is devoted to the danger that international intelligence sharing can be a means to short-circuit restraints on intelligence services in domestic law and also to provisions designed to protect information about intelligence cooperation from public disclosure. The importance of domestic legal provisions concerning the approval and review of international intelligence cooperation is dealt with in greater detail in Chapters 6 and 7. The chapter concludes by considering the inclusion of safeguards for human rights in domestic legislation and policy.

5.2 Relevance of regulating international intelligence cooperation in domestic law

In modern democracies, intelligence services are creatures of law – usually legislation made by the parliament– and so questions concerning the extent of their powers and control of them are legal questions rather than merely political ones. (Chapter 8 discusses the ways in which questions concerning intelligence cooperation can come before the courts). The topic of international intelligence cooperation, however, is often addressed through policy directives, and countries may legitimately take different approaches to the level of detail contained in primary legislation. Nonetheless, there are some fundamental matters that ought to be dealt with by legislation, even if in a particular state they are further elaborated in policy documents.

The inclusion of the authority for intelligence services to engage in necessary cooperation with foreign states in a domestic legal framework makes clear that this cooperation has democratic legitimacy. Consequently, even where detailed ministerial directives govern international intelligence cooperation, it is important that there is a clear legal basis for such guidelines and that they do not contradict the legislation. The legislative mandate of each of the intelligence services should, therefore, specify the general purposes for which intelligence can lawfully be gathered and used (regardless of whether it accessed through cooperation or other methods) and the main conditions to be met where the executive authorise cooperation.

In many countries, intelligence services have only been brought under effective legal and democratic control in recent decades. The principle of legality requires that this control should not be side-stepped by permitting a service to use cooperation to obtain information that it could not lawfully collect within its jurisdiction or the outsourcing to partners of activities that it could not undertake lawfully (see also Chapter 3). Legislation covering international intelligence cooperation can help guard against these risks. Safeguards should be incorporated to prevent the use of intelligence sharing, for example, in a way that circumvents controls in domestic law or a state's obligations under human rights law, and set down purposes for which intelligence cooperation cannot be used

Furthermore, the need for domestic legislation governing intelligence cooperation is underlined because of the obligations in international law. As we have seen in Chapter 4, there is a body of international law, especially human rights law, that binds states and their institutions, including intelligence services. A number of international human rights obligations are subject to national security limitations,[1] but states can only claim the benefit of such limitations for practices "prescribed by law" or "in accordance with law."[2] These clauses refer to domestic law. In the absence of legislation that can satisfy the test of being "in accordance with law," various aspects of international intelligence cooperation will be unlawful under international human rights law. For example, transfers of personal data constitute an interference with the right to respect for private life under Article 8 ECHR (or Article 17 of the ICCPR) and thus require a legal basis. The *UN Special Rapporteur for Promotion and protection of human rights and fundamental freedoms while countering terrorism* has raised concerns about the practices of sharing with foreign intelligence

services information concerning an individual's communications without the protection of a publicly accessible legal framework and adequate safeguards, and of systematically routing data collection and analytical tasks through jurisdictions with weaker safeguards for privacy. The Special Rapporteur concludes that such practices make the operation of the surveillance regime unforeseeable for those affected by it and are, therefore, incompatible with article 17 of the Covenant.[3] Despite that, as Chapter 4 has explained, there are very limited legal provisions on the sharing of information with foreign partners or on accessing data directly from foreign partners, and there is, therefore, a need from the point of view of international law for national legislators to address these questions.

A lack of domestic legislation (or indeed excessively vague legislation)[4] authorising intelligence cooperation, which may interfere with human rights, is potentially problematic. There is also a risk of exposing individual officials to legal liability for forms of intelligence cooperation that may involve criminal offences (for example, complicity in torture) if a clear framework for cooperation which complies which complies with international standards does not exist.

The limitations of a domestic legal framework for international intelligence cooperation must be recognised. As noted above, it is probably undesirable to seek to cover every aspect of cooperation in legislation, for example, because of the need to keep some forms of cooperation secret, and some more detailed guidelines and directions can be left to the authority of the government. Insofar as international intelligence cooperation takes place abroad, the actions of a state's services will be limited by their governing legislation but other general aspects of the legal system may not apply extraterritorially.[5] Moreover legislation cannot regulate the conduct of intelligence partners as such. The only ways that laws can address concerns over human rights or other abuses by intelligence partners are by procedural controls concerning prior scrutiny of which intelligence partners to cooperate with or review of the provenance of information received as a result of cooperation (see Chapter 6 for discussion of these). Neither of these is complete or perfect.

Furthermore, like intelligence services, oversight bodies are creatures of the legislation from which they derive their mandate. It is, therefore, important for accountability that the legislative mandate of bodies that oversee the intelligence services, whether a parliamentary committee or expert body, should make clear that their role and powers extend to the relevant intelligence cooperation and activities of the services they oversee. The same applies to executive bodies. While much of the control and direction of the services will take place through ministerial and other policy directives, the law governing the intelligence services should establish effective controls for approval of international intelligence cooperation, periodic review of international intelligence cooperation, budget controls, and auditing procedures. This establishes a basis for the political control of services and is an aid to laying down a clear chain of accountability.

In practice, the treatment of international intelligence cooperation in domestic legislation varies between states in the depth and levels of regulation, and in a number of states the legislation fails to deal with even the basic matters described above. Although constitutional differences play a role, these variations are not always the result of conscious deliberation

by legislators. The omission of the topic of international intelligence cooperation from legislation in some countries[6] may be due simply to a lack of awareness in earlier decades on the part of legislators of its significance – something that has only achieved public prominence in the last decade or so. Such an omission is, however, undesirable; it does not significantly add to operational secrecy but nonetheless creates the impression that cooperation is either beyond the mandate of the services and/or a part of national security activity that cannot be publicly acknowledged. Omission also makes it harder for oversight bodies to examine aspects of international intelligence cooperation involving the services under their jurisdiction.

5.3 Treatment of international cooperation in security and intelligence legislation

As noted above, legislation in different countries adopts a variety of approaches. These range from legislative silence (with cooperation undertaken on the basis of broad legislative authorisation to engage in operations), to broad authorisation of cooperation in the mandates of intelligence services, to (albeit more rarely) the inclusion of specific conditions or safeguards that apply to certain forms of cooperation.

In countries whose security and intelligence legislation does explicitly deal with international cooperation, there is a distinction between those laws that permit the services to engage in cooperation (for example, in Denmark, Estonia, and Hungary) and those where it is their duty to do so (for example in Belgium, Bosnia and Herzegovina, and Luxembourg). This is a formal distinction but arguably not an especially significant one since under either arrangement there is a legal discretion over the choice of intelligence partners. Some examples of provisions of this kind are given in Box 5.1 below.[7]

To summarise: legislators have a proper role in delineating the underlying principles and parameters of intelligence cooperation with foreign states, as well as the allocation of authority for approval and oversight of cooperation. The discussion above has identified several principles that parliamentarians, in particular, can follow in establishing an appropriate general legislative framework for international cooperation by intelligence services in a manner consistent with their own mandates and with the state's human rights obligations.

Recommendation:

The legislative mandate of each of the intelligence services should specify the general purposes for which intelligence can be lawfully be gathered and used (regardless of whether accessed through cooperation or other methods), the method by which it can be accessed and the main conditions to be met where the executive authorise cooperation.

Box 5.1: Legislative provisions authorising or requiring international cooperation[8]

State	Operative Provision
Denmark	The Danish Defense Information Service (DDIS) may use cooperation with foreign partners to get information useful to the national defence. (Act of 27 February 2001, as amended in 2006)
Estonia	The two security authorities - the State Information Service and the Security Police Board – "may exchange collected information with foreign services or international organisations if this is necessary to ensure or enhance national security." (Security Authorities Act of 2000 (as amended in December 2003)
Hungary	The National Security Bureau and the Special Service for National Security are permitted "to cooperate with foreign intelligence services on the basis of international agreements and arrangements." (CXXV 1995 Act §28)
Bosnia and Herzegovina	"[T]the Agency shall exchange intelligence and develop other types of co-operation with intelligence and security services in other states and other foreign and international institutions for the purpose of performing those tasks." (Article 6 of the 22 March 2004 Act on the Intelligence and Security Agency)
Luxembourg	The *Service de renseignement de l'Etat Luxembourgeois* (SREL) is mandated "to entertain an efficient cooperation with… foreign intelligence and security services." (Article 3 (1) of the 15 June 2004 Act)
Belgium	The *Sûreté de l'Etat/Veiligheid van de Staat*, the security service, and the *Service général de renseignement et de la sécurité (SGRS)/Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht*, the military intelligence service "have to maintain a collaboration with foreign intelligence and security services." (Article 20 §1 of the 30 November 1998 Act)
Greece	The National Intelligence Service (EYP-NIS) has the power "to cooperate with relevant Services of other countries and international organizations for the more effective performance of its duties." (Article 4-9 of the Act of 3 March 2008)
France	The *Direction Centrale du Renseignement Intérieur* (DCRI) "maintains necessary liaisons in its area of responsibility with French or foreign services and bodies, without prejudicing existing norms governing international police cooperation." (Decree of 27 June 2008, Art. 3)

Legislation should set down purposes for which intelligence cooperation cannot be used. Bearing in mind the risk that cooperation could be used by intelligence services to participate in activities beyond those authorized in their mandate or to gain access to material that they are not authorized to collect (see further, Chapter 3), safeguards against potential circumvention of controls are needed. These should include legislation to prevent the use of intelligence sharing in a way that circumvents controls in domestic law (including oversight arrangements) or a state's obligations under human rights law. There is a case, too, for more specific protections against circumvention of legal limits to intelligence gathering or surveillance, which is addressed in section 5.6 ("Human Rights Safeguards").

As noted above, there is a risk that cooperation could be used in a way that allows for obtaining of information that an intelligence service is not itself permitted to collect or to outsource illegal activities. While it is likely that any service that intentionally acted with this objective would be breaking the law in any event, and (as discussed in Chapter 4) it will be liable in international law according to the principles of state responsibility, there is, nevertheless, a strong case for the inclusion in domestic legislation of an explicit prohibition of outsourcing illegal activities to foreign partners. Equally, the executive should be prevented from directing services to use cooperation in this way. Legislation may contain safeguards against the avoidance of the controls that apply in domestic law through cooperation with foreign services or concerning the types of information that may be shared or the purpose of doing so, as recommended by a 2010 report to the UN Human Rights Council by the *Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while combating terrorism*.[9]

Recommendation:

Legislation should prohibit intelligence services from using 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.

5.4 Protection of information relating to international intelligence cooperation

It is common to find the confidentiality of international intelligence cooperation protected by legal provisions prohibiting disclosures of classified information, especially where countries are sharing information on the basis of mutually agreed arrangements for preventing disclosure. For example, in the United Kingdom, it is an offence for a civil servant or government contractor to make an unauthorised disclosure of material damaging to international relations.[10] The 1989 Act also covers (in section 6) a damaging disclosure of information relating to security, defence, or international relations that has been communicated in confidence by the UK government to another state or international organisation.[11] States that do not have legislation of this kind may, nonetheless, treat disclosures as serious offences – such as espionage and assisting the enemy.[12] Moreover, civil remedies such as breach of confidence may also be employed to deter disclosures. Additionally, courts in many countries protect information about liaison by legal doctrines that prevent certain kinds of sensitive evidence about intelligence matters on public interest grounds (for example, state secrets doctrine or public interest immunity) - as has happened in the US, UK and Italy for example. In some states, legislation governing intelligence oversight bodies contains either express or implied limitations that inhibit oversight or review of arrangements made with the intelligence services of other countries; these are discussed in Chapter 7.[13]

Freedom of information or privacy legislation also commonly contains an exception where disclosure of the information would be damaging to international relations and specific protections for information received in confidence from foreign governments and services.[14] For example, in Canada, the Access to Information Act (Section 13) contains a mandatory exemption for information received in confidence from a foreign government.[15] Section 15 of the Act contains further relevant exemptions for intelligence for diplomatic correspondence with foreign states or international organisations, and for information "relating to the communications or cryptographic systems of Canada or foreign states used for the conduct of international affairs, for the defence of Canada or any state allied or associated with Canada." Similarly in Australia, s. 33(1) of the Commonwealth Freedom of Information Act 1982, exempts documents that "could reasonably be expected' to damage security, defence or international relations of the Commonwealth or would divulge any information or matter communicated in confidence by or on behalf of a foreign government, an authority of a foreign government or an international organisation."

Where exchanges of information between the security and intelligence institutions of different countries take place behind a protective wall of statutory duties and exemptions such as these, it is all the more important that overseers (including information and data protection commissioners) are able to examine the nature of the activity and that they have access to all relevant information when investigating such matters.

While, as noted above, there is an important public interest in restricting access to information concerning sensitive aspects of intelligence cooperation, legislative restrictions of this kind can inhibit informed discussion of procedural and policy aspects

that are legitimate matters of public debate. Independent oversight committees, whose role is discussed further in Chapter 7, also have an important role in detecting problems at an early stage before they give rise to wider concerns. The recent large-scale releases of US-derived material detailing intelligence cooperation, as a result of WikiLeaks, and the allegations derived from the disclosures of Edward Snowden have raised public awareness of intelligence cooperation, but it has also been argued that they may also cause long-term damage to the intelligence effort of the countries.[16] There is still, therefore, a case to be made about the need for secrecy about intelligence sources and methods, including certain aspects of intelligence cooperation. Nevertheless, this cannot justify the use of secrecy to prevent the bringing to light of human rights violations.[17]

Secrecy should not, however, be based solely on harm to international relations but also require that such harms be balanced against the public interest in disclosure. This would mean disclosure could only be prevented under freedom of information or punished under official secrecy legislation if the public interest in non-disclosure outweighed it in disclosure. Such an approach has two important implications. Firstly, it is context and fact-sensitive and so excludes blanket-rules that prohibit all disclosures simply because they concern the topic of international intelligence cooperation. Secondly, it denotes a role for courts and other independent institutions (such as information commissioners) in determining where the balance of public interests lies in relation to particular disclosures. Thus, in the case of the Canadian Access to Information Act referred to above, in order to establish that section 13 has been correctly applied, it is possible for both the Information Commissioner and the Federal Court to examine the material in question. In Australia, the courts have determined that the contemplated damage by the decision-maker who withholds disclosure must be reasonable, rather than irrational, absurd, or ridiculous.[18]

As these examples show, legislators have a role of play in drawing a line between these competing public interests. The Open Society Justice Initiative has recently promulgated a set of Global Principles on National Security and the Right to Information ("The Tshwane Principles")[19] arrived at after an extensive process of enquiry and consultation with experts and NGOs to guide law-makers in this field. The Principles focus on the need not to suppress information relating to violations of human rights and recognise a legitimate case for protecting information concerning national security supplied by a foreign state or inter-governmental body with an express expectation of confidentiality, as well as other diplomatic communications concerning national security.[20]

However, they also suggest a number of pre-conditions (see Box 5.2)

Box 5.2: "The Tshwane Principles" and international intelligence cooperation information

Principle 4: Burden on Public Authority to Establish Legitimacy of Any Restriction
(a) The burden of demonstrating the legitimacy of any restriction rests with the public authority seeking to withhold information.

(c) In discharging this burden, it is not sufficient for a public authority simply to assert that there is a risk of harm; the authority is under a duty to provide specific, substantive reasons to support its assertions.

Principle 5: No Exemption for Any Public Authority
(b) Information may not be withheld on national security grounds simply on the basis that it was generated by, or shared with, a foreign state or inter-governmental body, or a particular public authority or unit within an authority.

Principle 9: Information that Legitimately May Be Withheld
(a) (v) Information concerning national security matters that was supplied by a foreign state or inter-governmental body with an express expectation of confidentiality; and other diplomatic communications insofar as they concern national security matters.
It is good practice for such expectations to be recorded in writing.

Principle 10: Categories of Information with a High Presumption or Overriding Interest in Favor of Disclosure
Some categories of information, including those listed below, are of particularly high public interest given their special significance to the process of democratic oversight and the rule of law. Accordingly, there is a very strong presumption, and in some cases an overriding imperative, that such information should be public and proactively disclosed.

Information in the following categories should enjoy at least a high presumption in favor of disclosure, and may be withheld on national security grounds only in the most exceptional circumstances and in a manner consistent with the other principles, only for a strictly limited period of time, only pursuant to law and only if there is no reasonable means by which to limit the harm that would be associated with disclosure.

(A). Violations of International Human Rights and Humanitarian Law

(1.) There is an overriding public interest in disclosure of information regarding gross violations of human rights or serious violations of international humanitarian law, including crimes under international law, and systematic or widespread violations of the rights to personal liberty and security. Such information may not be withheld on national security grounds in any circumstances.

(2) Information regarding other violations of human rights or humanitarian law is subject to a high presumption of disclosure, and in any event may not be withheld on national security grounds in a manner that would prevent accountability for the violations or deprive a victim of access to an effective remedy.

Recommendation:

Freedom of information or official secrets legislation should only prevent disclosure of information concerning international intelligence cooperation if the public interest in non-disclosure outweighs that in disclosure.

5.5 Procedural safeguards and international cooperation

In order to mitigate some of the potential risks of international intelligence cooperation, some states have requirements for procedural safeguards, concerning the process of approval and authorization.[21] Legislation may also provide for political approval of international cooperation agreements or require agreements to be shown to an outside review body. For example, the Canadian Security Intelligence Service Act 1984, section 17(2) requires that the Security Intelligence Review Committee be given copies of all CSIS agreements with foreign governments and international organizations. The provisions in the Netherlands from the Intelligence and Security Services Act 2002, Art. 59 (Box 5.3) are an especially clear example of a procedure of this kind.[22]

Box 5.3: Authorising international cooperation in the Netherlands

1. The heads of services are responsible for maintaining relations with the appropriate intelligence and security services of other countries.
2. Within the context of maintaining relations…. information may be provided to these services for the purpose of the interests served by these services, in so far as:
   a. these interests are not incompatible with the interests served by the services, and
   b. a proper performance of the duties does not dictate otherwise
3. [omitted]
4. Within the context of maintaining relations… and upon a written request to that end also technical and other forms of assistance may be rendered to these services for the purpose of the interests to be served by these services, in so far as:
   a. these interests are not incompatible with the interests served by the services, and
   b. a proper performance of the duties is not incompatible with the provision of this form of assistance.
5. A request for support… must be signed by the appropriate authority of this service who has the power to do so and must contain an accurate description of the required form of assistance and the reason why this assistance is considered desirable. The assistance requested shall only be granted if the relevant Minister has given permission for this.

Requirements of this kind have a number of benefits. They establish a clear framework for approval of cooperation activities. They can help to ensure that cooperation is aligned with the government's foreign policy, defence, security, and diplomatic objectives and does not unwittingly undermine or contradict these. They ensure that political overseers have an understanding of the arrangements that the state's services have with partners. They allow for scrutiny to take place of any risks of particular partnerships at an appropriate political and managerial level. The benefits of these types of legislative provisions, with examples from different countries and related approval, risk assessment, and reporting procedures are discussed in greater depth in Chapters 6 and 7.

Recommendations:

Legislation should provide for the procedure for approval of international intelligence cooperation agreements by the executive (for example, by a specified minister responsible for the intelligence service).

Procedural requirements should also include consideration of the human rights record of intelligence services with which information exchanged, so that appropriate safeguards can be put in place if necessary.

As noted above, an obligation to record cooperation activities strengthens accountability and review. Record-keeping obligations help to ensure proper accountability for intelligence cooperation activities and counter the danger that cooperation might be used in part for reasons of plausible deniability. A well-developed duty of this kind exists in Estonian law (see Box 5.4 below), and a similar statutory obligation can be found in legislation governing the Hungarian services.[23] There is also a duty in some countries to inform review bodies of formal cooperation agreements, as in the Canadian legislation mentioned above - this is a topic addressed further in Chapter 7.

Box 5.4: A duty to record cooperation activities: Estonia

Section 34. Exchange of information with foreign states and international organisations: "A security authority may exchange collected information with foreign services or international organisations if this is necessary to ensure or enhance national security on the basis of an international agreement. Unless otherwise prescribed by the international agreement, such exchange of information shall take place in writing."

§ 26. Transmission of state secrets to foreign countries and international organisations: "The State Chancellery and security authorities may transmit information classified as a state secret to foreign countries or international organisations in the cases and pursuant to the procedure prescribed by the Security Authorities Act if protection against disclosure of the information transmitted is guaranteed by an international agreement."[24]

Recommendations:

The legislative mandates of bodies that oversee the intelligence services (including parliamentary committees, non-parliamentary expert bodies, and, where their mandate includes the services, data protection and information commissioners, ombuds institutions and human rights commissions) should make clear that their role and powers extend to relevant intelligence cooperation and activities of the services they oversee.

Legislation should include provisions that oblige the service and/or executive to inform the intelligence oversight body about international intelligence cooperation agreements.

Legislation should include provisions on the duty of record keeping for international intelligence cooperation, in particular, concerning the exchange of information with foreign partners.

5.6: Human rights safeguards

The need for legislation in order to provide a legal basis for some forms of international intelligence cooperation that constitute an interference with human rights, particularly privacy, has already been explained in Chapter 4. The danger that international cooperation may undermine human rights protections, by side-stepping the balanced grant of powers by legislators to intelligence services, has also been referred to in Chapter 3. Recognising these dangers, a number of states have taken steps to embody safeguards designed to protect the fundamental rights of individuals during the course of international intelligence cooperation, some of which are described below.

While some matters require a clear legal framework because of international law requirements, not all questions in this field, however, are necessarily appropriate for intelligence legislation or indeed legislation at all. As explained in Chapter 4, some of the relevant international requirements are of general application – especially the protections against torture, inhuman and degrading treatment, arbitrary detention and enforced disappearance – and states have general obligations to legislate to provide the necessary safeguards in their laws governing criminal offences, criminal procedure, and evidence. These laws apply to everyone (including officials from the services) and, consequently, we do not address these here. Other questions may be more appropriately dealt with as a matter of political accountability, and legislation – if it is relevant at all - will provide only a skeleton for the development of ministerial directives. In other areas, legislation may be too rigid a response where there is need for flexibility, for example, to ensure the ability to adapt to rapid technological change. Recognising that human rights safeguards can, in some instances, take a variety of forms, the International Commission of Jurists Eminent Jurists Panel has advocated that:

> States should establish clear policies, regulations and procedures covering the exchange of information with foreign intelligence agencies. Where such procedures exist, by way of binding instruments or understandings, they should be reviewed in light of all relevant human rights standards. In particular, information should never be provided to another state where there is a credible risk that the information will cause or contribute to serious human rights violations.[25]

Bearing the above factors in mind, the discussion here focuses on the need to regulate in domestic legislation information sharing between services. As explained in Chapter 4, the sharing of information between services containing personal data engages privacy rights, and so it must be specifically authorised by national law.

The *UN Special Rapporteur for Promotion and protection of human rights and fundamental freedoms while countering terrorism* has raised concerns about the practices of sharing with foreign intelligence services. These relate to the lack of a publicly accessible legal framework and adequate safeguards to protect sharing of information concerning an individual's communications and to the systematic routing of data collection and analytical tasks through jurisdictions with weaker safeguards for privacy. The Special Rapporteur concludes that such practices make the operation of the surveillance regime unforeseeable for those affected by it and are, therefore, incompatible with article 17 of the Covenant.[26] Despite that, as Chapter 4 has explained, there are very limited legal provisions on the sharing of information with foreign partners or on accessing data directly from foreign partners. Therefore, from the point of view of international law, there is a need for national legislators to address these questions. The discussion below deals first with the need for legislation governing the supply of information by services to their partners, before dealing with the need for legislation concerning information received from intelligence partners, and finally the question of accessing data directly from foreign partners (in the case of bulk or untargeted surveillance).

CONTROLS ON THE SUPPLY OF INFORMATION

One type of safeguard expressly protects interests in exchanges involving personal data for information outgoing to foreign intelligence services. As explained in Chapter 4, the supply of personal data in this way constitutes an interference with the right of privacy protected by international human rights law. The supply of such information by an intelligence service, therefore, needs to be governed by legislation that deals with the reasons why information is shared, which are themselves compatible with legitimate aims, necessary and proportionate.[27] Box 5.5 gives some examples of such legislative controls on the supply of information, from Slovenia, Bosnia and Herzegovina, and Germany.

Box 5.5: Exchanges of personal data and international intelligence cooperation

State	Operative Provision
Slovenia	"When the Agency (the Slovene Intelligence Security Service, 'SOVA') forwards personal data to foreign intelligence and security services in accordance with this Act, it shall obtain in advance the guarantees that in the state to which the data are forwarded the personal data privacy is regulated and that the foreign intelligence and security service will use personal data only for the purposes defined by this Act." (Act on Slovene Intelligence and Security Agencies 1999, Article 12)
Bosnia and Herzegovina	"The Agency may only provide foreign security and other appropriate services with data regarding citizens of Bosnia and Herzegovina on the basis of information that the citizen poses a danger to the security of Bosnia and Herzegovina, the receiving state or a broader danger to regional or global security. "The Agency may not provide information regarding citizens pursuant to the preceding paragraph unless it has reasonable assurance that the recipient will provide the data with the same level of protection as provided in Bosnia and Herzegovina." (Law on the Intelligence and Security Agency of Bosnia and Herzegovina, 2004, Article 65)
Germany	"The Agency (the BfV – an domestic intelligence service) may provide foreign security and other appropriate foreign services, as well as supra and international organisations, with data regarding citizens, provided that: • The supplying of this data is essential for the pursuit of its duties or because prevailing security interests of the receiving institution necessitate this. • The supplying of information ceases when this would run counter to the predominant foreign concerns of the Federal Republic of Germany or where the pre-eminent interests of the affected private persons deserve to be protected. • The supplying of data ought to be recorded in public files The beneficiary is to be instructed that the information is transmitted on the understanding that the data may only be used for the specific purpose for which it was sent. The Agency reserves the right to request information on the usage of data by the beneficiary."[28]

Such legislative duties provide a basic framework, but they require elaboration by policies governing exchanges of information with foreign intelligence partners. For example, in practice, the use of caveats (conditions restricting the use of information shared with a partner intelligence service) is widespread when intelligence is supplied to an intelligence partner.[29] These are not a matter for legislation, as they are not legally enforceable. Their contribution is dealt with in Chapter 6, together with the implications for overseers. Box 5.6 describes the arrangements in Norway in order to illustrate the manner in which legislation can provide a framework for oversight of information exchanges.

Box 5.6: Information exchange in Norway[30]

Pursuant to Section 3 of Act No 11 of 20 March 1998 relating to the Norwegian Intelligence Service (NIS), referred to hereafter as "the Intelligence Service Act", the service "may establish and maintain intelligence cooperation with other countries." The NIS is a foreign intelligence service.

The EOS Committee oversees the service's exchange of information with foreign parties, primarily by keeping informed about the content of NIS archives and the service's communications system for information exchange with cooperating foreign services, and by inspecting the archives.

The Committee checks that personal data are only disclosed to cooperating services following a concrete assessment in each individual case of whether there is a basis for disclosure. In this connection, the Committee also oversees that NIS complies with the requirement set out in Section 4 of the Intelligence Service Act that the service shall not on Norwegian territory "monitor or in any other covert manner procure information concerning Norwegian physical or legal persons."

NIS must also continuously assess the receiving state's attitudes to and respect for fundamental human rights when the service exchanges personal data or other information, including when information is shared as part of Norway's participation in international operations.

Recommendation:

Legislation should govern the supply by an intelligence service of information containing personal data to a foreign service. The legislation should prescribe when and what information may be shared in a manner consistent with the state's human rights obligations (i.e. for legitimate aims and only where necessary and proportionate to those aims).

CONTROLS OVER INCOMING INFORMATION

In its 2007 Report on Democratic Oversight of the Security Services in Council of Europe States, the Venice Commission has suggested that where information is received from a foreign intelligence service or international agency, it should generally be held subject both to the controls applicable in the state of origin and those standards which apply under domestic law.[31] Ideally, this would mean information being subject to the oversight mechanism in full in the state that receives foreign-derived intelligence. As explained in Chapter 4, the processing, analysis, and communication of incoming material within the receiving state's jurisdiction are governed by its human rights obligations. As a minimum, therefore, the treatment of incoming information containing personal data needs to be governed by legislation dealing with the reasons why information is retained or destroyed, processed, and disseminated, which are themselves compatible with legitimate aims and necessary and proportionate.[32]

Recommendation:

Legislation should govern the receipt by an intelligence service of information containing personal data from a foreign service. The legislation should prescribe when and what information may be retained, destroyed, processed, or disseminated in a manner consistent with the state's human rights obligations (i.e. for legitimate aims and only where necessary and proportionate to those aims).

CONTROLS OVER UNTARGETED OR BULK SURVEILLANCE

As part of the Snowden revelations, it has been widely suggested that some intelligence services may request foreign partners to collect intelligence on their territory (or communications originating from there) if national legal requirements on the use of intrusive collection methods would prohibit them from collecting the information themselves or would make it particularly burdensome.[33] In general, there is a clear case for an absolute prohibition on the deliberate use of intelligence sharing to evade legal obligations pertaining to the collection of information, as the discussion of the risks of circumvention (above) argues. Intelligence services should not be permitted to circumvent legal requirements through international intelligence cooperation. Equally, intelligence services should not be permitted to collect information on behalf of other services for the purpose of bypassing regulations which would prohibit or restrict the collection of this information by these services.

In response to the Snowden revelations, both the German and UK intelligence services have issued clear and emphatic denials of deliberate resort to information sharing in the manner alleged.[34] The possibility of passive receipt of such information through access to material collected by partners through untargeted surveillance has, however, been conceded in the UK. This led to a finding by the UK Investigatory Powers Tribunal (IPT) that GCHQ was acting unlawfully, at least until a policy document detailing the controls on this practice was made public in December 2014 as part of proceedings. The disclosure of the policy satisfied the IPT that arrangements for GCHQ to access such material in the

future were sufficiently clear so as to be foreseeable for the purpose of the "authorised by law" test under Art. 8 of the ECHR.[35] That finding is controversial and is likely to be tested in forthcoming challenges before the European Court of Human Rights. In any event, it is clearly preferable from the point of view of the rule of law for the safeguards on access to untargeted surveillance material collected as a result of intelligence cooperation to be contained in legislation rather than policy documents. The Council of Europe Venice Commission has proposed that:

> A suitable safeguard…. to provide that the bulk material transferred can only be searched if all the material requirements of a national search are fulfilled and this is duly authorized in the same way as a search of bulk material obtained by the signals intelligence agency by its own techniques.[36]

This proposal is framed against the assumption that it is desirable for legislation to govern searches of bulk material collected by intelligence services' untargeted surveillance. Some countries regulate the authorization of keyword searches under warrant-type procedures in legislation, for example.[37]

Recommendations:

Legislation should make it clear if services utilise liaison/international intelligence cooperation to gather information about persons within their jurisdiction, then they should be required to meet the same requirements as would apply when seeking that information themselves (i.e. concerning permissible purpose, threshold of suspicion, and independent authorisation).

In particular, where bulk material is transferred by a foreign intelligence or signals intelligence agency, the recipient agency should only be permitted by legislation to search it if all the material requirements of a national search are fulfilled and this is authorized, in the same way as a search of bulk material directly obtained by the recipient agency itself.

Endnotes

1. In particular, for Council of Europe states, Article 8 of the European Convention on Human Rights (ECHR).
2. The European Court of Human Rights has treated "[I]n accordance with the law" as requiring both that there should 'some basis in domestic law' for the restriction in question and that it meets the test of 'quality of law'. The latter test requires it 'should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law." (*Weber and Saravia v. Germany*, no. 54934/00, 29 June 2006). Breaches of Article 8 have been found by where the member states either have no legislation governing their intelligence services or the legislation is silent on matters such as the collection or storage or personal data (for example, *V v. Netherlands*, no. 14084-88/88, 3 December 1991). Under the 'quality of law' test the law must give an 'adequate indication' to citizens of when it can be used and discretion granted to the executive must not be 'unfettered'. The Court will check that it states sufficiently clearly, for example, the procedure 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 may or must be erased or the tapes destroyed (see, for example, the detailed analysis of the German G10 law in *Weber and Saravia v. Germany*, admissibility decision ECtHR, 29 June 2006).
3. UN Special Rapporteur for Promotion and protection of human rights and fundamental freedoms while countering terrorism, *Annual report of the Special Rapporteur to the General Assembly*, A/69/397, para. 44.
4. See note 2 above.
5. Although some oversight bodies may apply domestic law standards by analogy to extra-territorial activities.
6. It is not, for example, mentioned in the following: Act of 22 December 1990 for the Bundesnachrichtendienst (BND) in Germany; Decree of 2 April 1982 for the Direction générale de la sécurité extérieure (DGSE) in France; Act of 23 July 2001 for the HeeresNachrichtenAmt (HnaA) in Austria; or Act of 30 July 2004 for the Security Information Service in the Czech Republic. See Philipp Hayez, "National oversight of international intelligence cooperation," in *International intelligence cooperation and accountability*, ed., Hans Born, Ian Leigh and Aidan Wills, (London: Routledge, 2011), 158.
7. And see Box 5.3, discussing the Netherlands' provision.
8. Philipp Hayez, "National oversight of international intelligence cooperation," in *International intelligence cooperation and accountability*.
9. UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Combating Terrorism, *Compilation of good practice on legal and institutional and measures that ensure respect for human rights by intelligence agencies*, A/HRC/14/46, 17 May 2010. Practice 35.
10. Official Secrets Act 1989, section 3. Note that in the UK the government had originally proposed no damage requirement should apply to disclosures of information received from foreign governments or international organisations because of the wider damage to the UK's standing in the international community that such disclosures would cause: *Reform of Section 2 of the Official Secrets Act 1911*, Cm 408 (1988), para. 51.
11. These provisions have been invoked several times recently because of sensitive disclosures by civil servants about cooperation, for example concerning the Iraq War: "Ex-GCHQ Woman Cleared Over Leak," *BBC News*, 13 November 2003; "'Brave' Official Praised for Leak," *BBC News*, 8 January 2008; "Official Cleared in Secrets Case," *BBC News*, 9 January 2008; "When Should a Secret Not be a Secret?" *BBC News*, 10 May 2007.
12. For example the prosecution and conviction of the US serviceman Bradley Manning over the Wikileaks disclosures. Manning was convicted in August 2013 of offences under the Espionage Act and sentenced to 35 years' imprisonment but acquitted of 'assisting the enemy'; "Bradley Manning sentenced to 35 years in Wikileaks case," *BBC News*, 21 August 2013.
13. In the UK, "information provided by, or by an agency of, the Government of a territory outside the United Kingdom where that Government does not consent to the disclosure of the information" is treated as 'sensitive information' under the Justice and Security Act 2013, Schedule 1. Paragraph 5.(c).
14. In some states, the security and intelligence services are exempt altogether from freedom of information and data protection legislation. In these instances, partner-derived intelligence will be exempt along with all other material held by the services. Arguably, exemptions (as opposed to the exceptions discussed in the text) are excessive since they prevent any form of independent review of the need to withhold information. See further: Ian Leigh, "Overseeing the Use of Personal Data," in *Overseeing Intelligence Services – A Toolkit*, ed., Hans Born and Aidan Wills, (Geneva: DCAF, 2012), 114-116.

15. Under s. 13.2 material may be disclosed if the government or institution concerned consents or itself makes the information public.
16. "Snowden leaks 'worst ever loss to British intelligence'," *BBC News*, 11 October 2013.
17. See "Tshwane Principles", Box 5.2 below.
18. Applying the 'reasonable expectation' standard: *Re Slater and Cox* (1988) 15 ALD 20, 26-7. (Regarding access to historical material on the Australian Secret Intelligence Service regarding Cambodia, Indonesia, West New Guinea and Singapore). *Re McKnight and Australian Archives* (1992) 28 ALD 95, 111 (Regarding material passed by the UK security services in confidence to ASIO). See further Chapter 8 below.
19. Finalized in Tshwane, South Africa, issued on 12 June 2013. These Principles were drafted by 22 organizations and academic centres in consultation with more than 500 experts from more than 70 countries at 14 meetings held around the world, facilitated by the Open Society Justice Initiative, and in consultation with the four UN special rapporteurs on freedom of expression and/or media freedom and the special rapporteur on counter-terrorism and human rights:
    - the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression,
    - the UN Special Rapporteur on Counter-Terrorism and Human Rights,
    - the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information,
    - the Organization of American States (OAS) Special Rapporteur on Freedom of Expression, and
    - the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media.
20. "Tshwane Principles", Principle 9 (a) (v).
21. For a helpful discussion see Kent Roach, "Overseeing Information Sharing" in *Overseeing Intelligence Services – A Toolkit*.
22. The Review Committee for the Intelligence and Security Services (CTIVD) has recommended a series of detailed procedural requirements for cooperation to supplement the statutory provisions: CTIVD, *Review report 22a on the cooperation by GISS with foreign intelligence and security services*, (The Hague, 2009), 43.
23. Act CXXV of 1995 on the National Security Services, section 46 (duty record data supplied); see also Ch. 6, discussing the Dutch and Norwegian provisions.
24. Security Authorities Act of 2000, as amended December 2003.
25. International Commission of Jurists Eminent Jurists Panel, *Assessing Damage, Urging Action*, (Geneva, 2009), 90; see also UN Special Rapporteur on protecting human rights and fundamental freedoms while countering terrorism, *Compilation of good practice on legal and institutional and measures that ensure respect for human rights by intelligence agencies*, Practice 31.
26. UN Special Rapporteur for Promotion and protection of human rights and fundamental freedoms while countering terrorism, *Annual report of the Special Rapporteur to the General Assembly*, A/69/397, para. 44.
27. Concerning the requirements of Art. 8 ECHR, see note 2 above.
28. Germany, Bundesverfassungsschutzgesetz [Federal Constitution Protection Act], 2002, Art. 19.
29. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (Arar Commission), *Report of the Events Relating to Maher Arar: Analysis and Recommendations*, (Ottawa: Canadian Government Publishing, 2006), 339-42.
30. Annual Reports of the EOS Committee 2003–2012. This box describes the position with regard to the Norwegian Intelligence Service. Information exchanges by the Police Security Service are also governed in detail by the Act No 4 of 4 August 1995 relating to the Police (sections 17 and 24), by Regulation No 920 of 19 August 2005 concerning the Norwegian Police Security Service, and by internal Guidelines for the processing of information. Implementation is overseen by the EOS.
31. Council of Europe, European Commission for Democracy through Law (Venice Commission), *Report on Democratic Oversight of the Security Services in Council of Europe States*, June 2007, 39-40. The Venice Commission noted that a weaker, alternative arrangement, may be to establish a system of certification. This would entail the oversight institution in the state supplying intelligence warranting that it has been collected and handled according to local standards of legality.
32. Concerning the requirements of Art. 8 ECHR, see footnote 2 above.

33. European Parliament, Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee), *Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*; Council of Europe, Committee on Legal Affairs and Human Rights of the Parliamentary Assembly (Rapporteur Pieter Omtzigt), *Mass Surveillance*, 2015.
34. Council of Europe, Committee on Legal Affairs and Human Rights of the Parliamentary Assembly (Rapporteur Pieter Omtzigt), *Mass Surveillance*, 2015, paras. 30-37.
35. *Liberty and others v. The Secretary of State for Foreign and Commonwealth Affairs and others*, Case Nos. IPT/13/77/CH; 13/92/CH; 13/194/C and 13/204/CH, [2015] UKIPTrib 13_77–H at 153-154.
36. Venice Commission, *Update of the 2007 Report on Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies*, CDL-AD (2015), para. 78.
37. Venice Commission, *Update of the 2007 Report on Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies*, CDL-AD (2015), paras. 214, 126-133, describing arrangements for authorization in Germany, the United States and Sweden. In the Netherlands see CTIVD, *Annual Report for 2013-14*, 16-17 discussing Arts. 26 and 27 of the Intelligence and Security Service Act 2002 and recommending the introduction of closer controls. In the UK, see proposals from the Independent Reviewer of Counter-Terrorism Legislation, *A Question of Trust- Report of the Investigatory Powers Review* (2015), 292-294.

Part III: Accountability of International Intelligence Cooperation

6

Internal and Executive Controls of International Intelligence Cooperation

6.1 Introduction

Members of intelligence services and especially senior managers play the preeminent role in determining how international intelligence cooperation is carried out, how risks are managed, and whether it is effective and lawful. Their actions have significant implications for the efficacy of external oversight and executive oversight and control; ultimately, the accountability of international intelligence cooperation begins with service managers and their staff. As consumers of intelligence, taskmasters, and holders political responsibility for the services, members of the political executive responsible for intelligence services are at the same time beneficiaries, controllers, overseers, and accountable for international intelligence cooperation. Like the intelligence services, they are subject to external oversight (by e.g. parliamentary and expert bodies – see Chapter 7) for their role in international intelligence cooperation.

This chapter will begin by addressing the role of intelligence services themselves, focussing on the internal controls that can be adopted to ensure that services reap the benefits of cooperation with foreign services, while also managing the risks associated with international intelligence cooperation (see Chapter 3). The second half of the chapter will consider the role of the executive (responsible ministers and their ministries/departments and collectives such as national security councils) in the control and oversight of international intelligence cooperation.

6.2 Internal controls

Intelligence services have the primary responsibility for making decisions about international intelligence cooperation. Within the confines of the legal framework regulating their work, the foreign policy of the government and the priorities established by ministers, service management is responsible for deciding how, when, and with which foreign services cooperation will take place. Although this guide emphasises the importance of executive control and external oversight of services' international cooperation, intelligence service staff play the leading role in ensuring international intelligence cooperation is legal, appropriate, effective, and accountable. Individual members of services (not overseers or members of executive) are present when critical decisions are made. For this reason, their values, ethics, and legal knowledge are of utmost importance. Excellent systems of executive control and/or external oversight count for little if services are not committed to pursuing their mission in an ethical manner in accordance with the law and the policies of the government. This observation applies to international intelligence cooperation as much as to any other part of their work.

This section will outline some of the procedures, checks, and regulations within intelligence services that help ensure that their cooperation with foreign services contributes effectively to the fulfilment of their mandate, complies with legal standards, and manages risks appropriately. Service managers are responsible for putting in place these procedures and, crucially, ensuring that their staff understand and comply with them.

RISK ASSESSMENTS

Services' risk assessment or due diligence processes are an indispensable mechanism for managing international intelligence cooperation. They help to reduce the possibility that cooperation will give rise to the various risks discussed in Chapter 3. Risk assessments should occur before entering into a cooperation agreement with a foreign service, before intensifying cooperation (e.g. by formalised processes for sharing personal data), as well as in specific instances of cooperation (e.g. a joint operation).

Risk assessments use predefined criteria to evaluate a foreign service in general, as well as to evaluate proposed instances of cooperation, such as the sending of tactical information on a particular person. As this guide has shown, the sending of personal data is a form of international intelligence cooperation that demands a particularly judicious risk assessment. With regards to individual cases of cooperation, possible benefits, as

well as risks are normally considered. In many cases, there will be compelling grounds for undertaking a particular form of cooperation, and there may be considerable uncertainty over whether identified risks are likely to crystallise. It is important to recognise the conditions of uncertainty, in which judgements are made in good faith but, subsequently, may turn out to be flawed.

The outcomes of risks assessments have important implications for:

a. Whether or not particular instances or forms of cooperation can proceed, including whether personal data can be shared with a foreign service.
b. The measures that should be taken to mitigate risks in a particular case. For example, a risk assessment may give rise to the conclusion that some personal data should be expunged or that the service needs to solicit written assurances regarding how information will be used.

An essential consideration for many forms of international intelligence cooperation is the possible impact that the cooperation will have on any individual concerned. Taking two examples from Chapter 3, it should be clear that, if it is known that someone is in detention overseas in a country with a poor human rights record, extreme caution should be exercised in sharing any information with the custodians. Similarly, if an intelligence service is known to make systematic use of practices that violate human rights, e.g. targeted assassinations or torture, very serious consideration should be given as to whether personal data should be shared with that service. Intelligence services and the executive need to adopt policies on what types and levels of risk should preclude cooperation (see e.g. Box 6.6, below), and what evidence of risk is required in such situations. These questions are likely to be answered differently across jurisdictions. Chapter 4 provides a detailed assessment of the international legal standards that should inform any such assessments.

Recommendations:

Intelligence service managers should put in place risk assessment processes for international intelligence cooperation that set out the factors which must be considered before undertaking particular types of cooperation. These processes adopted should take account of an intelligence service's domestic and international legal obligations.

Oversight bodies should verify that such processes exist and evaluate risk assessment policies and practices to satisfy themselves that relevant factors are considered.

What Factors Should be Considered in a Risk Assessment Process?

The specific factors that need to be addressed when deciding whether or not to cooperate with a foreign service vary depending on the type of cooperation and the operational context. However, it is possible to identify some general questions that services should address before engaging in cooperation. This is followed by two examples of assessment criteria used by the Dutch General Intelligence and Security Service [AIVD] (covering all forms of cooperation with foreign services) and the Norwegian Police Security Service [PST] (on sending information to foreign services).

When a service is considering a request for cooperation from a foreign partner or considering requesting the cooperation of a partner, the following general questions are commonly addressed:

1. Is there any cooperation agreement or MoU in place with the foreign intelligence service concerned? If so, does the proposed cooperation fall under the scope of this agreement? If it does not, are there any extenuating circumstances that would justify cooperation beyond the agreed framework?
2. Is the proposed cooperation consistent with the state's national security and strategic interests?
3. Would the proposed cooperation be consistent with current foreign policy?
4. Has legal advice been taken on whether the proposed cooperation can lawfully be conducted, including:
   a. If the request from a foreign partner requires the service to take action (e.g. placing someone under surveillance or using a particular selector/search term to gather data), would this action be permitted under domestic law?
   b. Would a request submitted to a foreign service involve it doing anything that would be unlawful on the requesting state's territory?
   c. Would a request submitted to a foreign service have the effect of enabling the requesting service to receive information which it either could not obtain under its own law or would require a warrant to obtain?
5. How important is the prospective gain from the cooperation?
6. Who might be affected by the proposed cooperation and what are the possible consequences for them, including for their human rights?
7. Could the proposed cooperation give rise to any action for which the service could be liable and/or with which your service would not wish to be associated?

Box 6.1: Summary of the Norwegian PST guidelines and practices on sending information to foreign services

The PST can disclose information to foreign police authorities, security or intelligence services in order to avert or prevent criminal offences or if it is necessary in order to verify information. Before doing so, the service must assess the following factors:

- The proportionality between the purpose of the disclosure and the (potential) consequences for the individuals concerned (including for their relatives).
- The quality and importance of the information.
- The human rights situation in the country.
- Where a specific request was received, the service will also examine the seriousness of alleged activities of the person about whom information is sought and the grounds of suspicion provided by the foreign service.

With regards to sending personal data, the PST must be able to demonstrate that it carried out such an assessment. This is something that the Service's oversight committee, the EOS Committee, regularly examines.

Box 6.2: Summary of the Dutch General Intelligence and Security Service's internal guidelines on cooperation with foreign intelligence and security services[1]

The AIVD is required to consider specific factors before entering into a cooperation relationship, intensifying a relationship or engaging in specific cases of cooperation. The CTIVD (AIVD's oversight body) has recommended that the assessment should include the following steps:

1. GENERAL RISK ASSESSMENT

For each foreign partner, the AIVD management should evaluate the following criteria. The outcome of this assessment will determine the possible scope of cooperation.

a. Democratic anchorage and respect for human rights

The Service must consider *inter alia* a (prospective) partner's political system; the position of intelligence services within that system; the statutory powers of the service concerned, independent oversight of the service; whether the country concerned has ratified international HR conventions and its record of adhering to these conventions; and any allegations about HR violations.

b. Tasks, professionalism, and reliability

This includes an examination of the mandate of a foreign service (e.g. external, domestic, or combined mandate); its specific powers including executive powers (i.e. powers of arrest and detention). *These factors are assessed because they have consequences for how shared information might be used. Professionalism and reliability are difficult to assess at the outset and have to be evaluated as a relationship develops.*

c. Advisability in the context of international obligations

The Service must act in accordance with the state's international obligations, and it, therefore, has to assess whether cooperation would further these interests or could give rise to a conflict of interests. In relation to cooperation with high-risk services, the service also has to assess whether ministerial approval must be sought.

d. Enhancing the performance of its statutory tasks

The Service is required to cooperate with foreign counterparts as part of its statutory mandate. It must assess whether cooperation would further the performance of its statutory tasks, and it must normally ensure that there are common interests underpinning cooperation.

e. Quid pro quo

The Service is permitted to cooperate with a foreign partner to support that partner's interests (as long as it does not contradict its own interests) with the assumption being that partners will return such favours. It must, however, avoid going too far, and it must keep track of the "*quid pro quo* balance." This can be relevant in deciding if and how to cooperate in given cases.

2. CASE-BY-CASE RISK ASSESSMENT

For individual (operational) cases/instances of cooperation, the AIVD should evaluate the specific interests involved and weigh the outcome of this (operational) assessment against the general assessment that determines the scope of cooperation with the foreign service. Should the specific operational interests require the AIVD to go further than what is permitted by the general risk assessment (above), thus giving rise to an exceptional situation, a reasoned decision on the matter should be taken at management level.

Acquiring the Relevant Information for Risk Assessments

Services specialise in gathering information and are well placed to gather the information necessary to assess their foreign partners. They have the duty to attempt to apprise themselves of information about the activities and methods used by (prospective) partners – open sources alone offer significant amounts of information in this regard. Nevertheless, evaluating a prospective partner can be particularly challenging because services may know very little about the service concerned. Where possible, services may wish to seek information from other entities in their own intelligence communities and other foreign partners. When evaluating the human rights records of foreign partners, it is also prudent to refer to the reports of foreign ministries, international organisations (such as the reports of UN special mandate holders and the Universal Periodic Review process), and reputable NGOs.[2]

Recommendations:

The executive should ensure that there is cross-government sharing of appropriate information on countries' human rights records as this assists services in undertaking risk assessments.

Oversight bodies should examine whether intelligence services' risk assessment processes take account of information from reputable NGOs and international organisations.

Database of General Assessments of Foreign Services

The Dutch CTIVD has recommended that it is good practice for services to conduct a general assessment for all cooperation partners.[3] This can be done by a foreign relations unit within the service or foreign ministry or a central intelligence coordination unit (where one exists) and be accessible by all relevant departments. Such assessments can provide a starting point from which prospective cases of cooperation can be assessed in more detail. Case officers have a vested interest in their own operations; while they may be well placed to consider the likely benefits of cooperating with a foreign partner, they may not the most appropriate party for assessing the risks attached to working with a given service.

ASSESSING INCOMING INFORMATION

All services have procedures for evaluating and verifying information they receive. This applies not only to information from foreign partners but all sources of information. Intelligence services are inherently suspicious and will be mindful of, for example, attempts to manipulate them through erroneous or embellished information. In view of this, services will generally seek to verify and corroborate incoming information.

It is important that assessments of the accuracy and reliability of incoming information also play close attention to any possible human rights concerns relating to the provenance of information. Concerns about the human rights "foot print" of incoming information go beyond the implications for reliability; they also include possible legal implications

of using such information. The Arar Commission recommended that assessments of incoming information from countries with poor human rights records should include "consideration of the general patterns of conduct of the country and not be limited to first-hand evidence of torture in specific instances."[4] While it may be unrealistic to expect that services will know whether incoming information was obtained in violation of human rights, it is imperative that retained information is flagged if it comes from foreign services with poor human rights records. Any information marked in this way should not serve as the basis for court proceedings, and only in exceptional cases would it be expected that action is taken on it that affects an individual's s legal rights, including adverse security assessments, travel bans, and surveillance. Where a services has grounds to believe that incoming information was obtained through torture or serious inhuman and degrading treatment, it should not be used for any purpose.

Recommendation:

Oversight bodies should review intelligence service decisions to request information from foreign services with poor human rights records. They should also examine policies and procedures for assessing the reliability of and recording/marking incoming information received from such services.

ATTACHING CAVEATS TO OUTGOING INFORMATION

Intelligence services often attach conditions to information they send to foreign partners – these are known as caveats (see Box 6.3 for examples). They are intended to restrict the use of information by the recipient,[5] and, more specifically, they "can serve to establish proper channels for clear communication about the use and distribution of the information subject to the caveat."[6] Services sending information use caveats primarily to protect their information (and indirectly their sources and methods) and to keep secret from third parties the fact that that they have shared information with the recipient. However, caveats can also make it less likely that outgoing information (especially personal data) will contribute to the violation of human rights. Indeed, inquiries into information sharing with foreign services have highlighted the failure to attach caveats to outgoing information as having contributed to actions that violated human rights.[7]

Caveats generally include assertions that the information should not, without the sender's express permission, be transmitted to a third party (i.e. restating the third party rule – see Chapter 7), used in legal proceedings, or used for taking executive action, such as making arrests. Services can supplement these conditions with more specific demands in situations where they have particular concerns. It is important that caveats are not only attached to outgoing information but also that they are worded in sufficiently clear terms, particularly with regards to defining how widely information may be shared in the recipient's government and precisely how it may be used.[8]

Caveats do not guarantee that information will not be used contrarily to the wishes of sending services, not least because the service attaching the caveat has no way of

ensuring that restrictions placed on the use of the information are respected. In practice, it is extremely difficult for services to be sure how their foreign partners use their information. Nor does the use of caveats reduce the need for services to undertake risk assessments (see above). They do, nevertheless, establish a written expectation regarding how information may be used. If discovered, a failure to comply with such undertakings may result in the recipient not receiving information in future.

Box 6.3: Examples of caveats that have been used by the Canadian Security Intelligence Service

CSIS internal policy requires that the appropriate caveat must be added to all information or intelligence disclosed in written or print form to any person, agency or department outside the Service.

This document is the property of the Canadian Security Intelligence Service. It is loaned to your agency/department in confidence. The information or intelligence contained in this document emanates from sensitive sources and no action may be taken on the basis of this information or intelligence which may jeopardize those sources. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator.

Our Service recognizes the sovereign right of your government to undertake reasonable measures under the law to ensure your public safety. Should you deem some form of legal action against the individual is warranted, our Service trusts that the individual will be fairly treated within the accepted norms of international conventions, accorded due process under law and afforded access to Canadian diplomatic personnel if requested. Furthermore, should you be in possession of any information that originated from our Service regarding the individual we ask that this information not be used to support the detention or prosecution of the individual without prior formal consultation with our Service.[9]

Recommendations:

Intelligence services should ensure that caveats are attached to information shared with foreign partners.

Caveats should set out in unambiguous terms the use to which that information may be put and with whom it may be shared.

Oversight bodies should review the standard caveats attached to outgoing information as well as intelligence service policies for monitoring adherence to caveats and addressing breaches of caveats by foreign services.

RELIABILITY ASSESSMENTS

Alongside caveats, it is good practice for services to attach reliability assessments to outgoing information. This assists the recipient in making an assessment of the information's value, and it may influence how they use the information. Sending unverified information without provisos to this effect can increase the risk that the information might be used

in violation of human rights. A person may, for example, be detained and interrogated following the receipt of information based on suspicion or conjecture. Recognising this, Norwegian regulations require the PST to inform foreign partners whenever outgoing information is unverified.[10] Intelligence is by its nature different from evidence (although in some cases it may be convertible into evidence). It is typically fragmentary, incomplete and difficult to assess, and will sometimes be sometimes wrong, and that needs always to be borne in mind by the receiving state.

Recommendation:

Reliability assessments should be attached to intelligence shared with foreign partners, particularly where it relates to identifiable individuals.

SEEKING ASSURANCES FROM FOREIGN SERVICES WHEN SENDING INFORMATION

Beyond caveats, a service sending information to a foreign partner may opt to demand specific assurances regarding how the information will (not) be used.[11] Services can seek such undertakings when they have concerns that information might, for example, be introduced into an unfair criminal trial or trigger the detention of a suspected terrorist's family. Assurances can offer better safeguards than caveats because they entail the would-be recipient making an explicit written commitment on the use of information, rather than simply being directed not to use information in a particular manner. Yet, in common with caveats, assurances are not a panacea and do not provide a guarantee that information shared will not be used in a manner that violates human rights. From a service's perspective, demanding such assurances from foreign partners can pose a problem for their relationships because it may be construed as demonstrating a lack of trust. Accordingly, this is an instrument that services may be reluctant to use too often.[12]

Recommendations:

Overseers should pay close attention to the use of assurances in situations where there exists a risk that outgoing information could be used in violation of human rights. Overseers should examine:

- whether assurances are sought,
- whether they are sufficiently detailed and credible,
- whether it is reasonable to reply on them, and
- whether mechanisms exist for ensuring that they are being adhered to.[13]

TRAINING

Given the pre-eminent role of individual intelligence officers in ensuring that international intelligence cooperation is conducted in an appropriate and lawful manner, as well as in a way that contributes to the legal mandate of their intelligence service, it is essential that that intelligence officers are given training in matters such as human rights considerations when sharing information, identifying and reporting concerns surrounding the treatment

of detainees by a foreign partner, as well as on the use of information by foreign partners. This is particularly important in view of the fact that officers will sometimes be working overseas and have to make their own decisions about cooperation that may have significant consequences. It may not always be feasible to consult with senior management and legal advisers at headquarters.

All staff should be fully acquainted with the prevailing internal, ministerial, statutory, and international legal provisions governing the work of the service, including cooperation with foreign services. Training should cover not only the relevant legal standards but also techniques for identifying and assessing benefits and risks to human rights. This would include training in how to conduct risk assessments and due diligence assessments on foreign partners, as well as how to identify human rights and take action to address human rights concerns that arise during cooperation with foreign partners.[14]

Recommendations:

Intelligence service personnel involved in international intelligence cooperation should be provided with training on the risks involved, including how to identify, report, and mitigate risks to human rights. Training should also include guidance on requirements for seeking authorisation from senior management and/or the executive, record keeping, and service obligations to external oversight bodies.

Overseers should evaluate services' training programmes and satisfy themselves that training on relevant aspects of international intelligence is not only is provided but is also understood by intelligence officers.

It is essential that training on ethics and compliance is not simply a "bolt on" to the core curriculum offered to, for example, new recruits. It must be an integral part of that core curriculum and managers must have refresher training. Training should include guidance on the role of overseers and members of oversight committees should, if possible, make themselves available to address groups from the services.

CLEAR AUTHORISATION PROCEDURES

It is important that services have clear procedures for authorising cooperation with foreign partners. These procedures should be outlined in internal regulations with the aim of promoting consistency. Establishing responsibility for making decisions (or delegating decision-making powers) in this area of a service's activity is important from the point of view of holding individuals to account for their decisions. Clear lines of decision-making authority also benefit rank and file intelligence officers because it gives them the assurance of knowing that their actions are underpinned by authorisations from nominated senior staff. This does not, however, relieve members of intelligence services of their responsibility to refuse to carry out directions that are manifestly illegal and that could give rise to individual legal liability.

As a general rule, the greater the risk or consequences of a proposed action, the more senior the level of decision-making authority required. Box 6.6 (below) provides the UK

example of a requirement for intelligence officers to consult senior staff whenever the risk of torture or cruel, inhuman and degrading treatment reaches a given threshold. Another example is the Canadian Ministerial Directive on Information Sharing with Foreign Entities requires that CSIS establishes "approval levels that are proportionate to the risks in sharing information with foreign entities." The Directive further stipulates:

> When there is a substantial risk that sending information to, or soliciting information from, a foreign entity would result in the mistreatment of an individual, and it is unclear whether the risk can be mitigated through the use of caveats or assurances, the matter will be referred to the Director for decision.[15]

Elsewhere, the Dutch AIVD requires that all decisions on the sharing of personal data be made by a senior manager.[16] Notwithstanding any role of ministers, service directors should always be involved in authorising the most high-risk forms of cooperation before they are passed on to ministers for final approval.

ENSURING PROPER DOCUMENTATION AND RECORDS KEEPING

Documenting all aspects of international intelligence cooperation is essential for enabling subsequent review of international intelligence cooperation activities and holding relevant persons to account for their performance of such activities.[17] It helps both services and their external overseers to identify any problems and make appropriate improvements to policies and practices. Overseers cannot effectively oversee services' cooperation with foreign partners if services do not keep comprehensive records. Illustrating the importance of record keeping, it has been reported in the context of ongoing Bundestag inquiries into the role of the NSA (and its cooperation with German intelligence services) that the BND failed to record all data passed on to the NSA following SIGINT collection requests (see Box 2.2 in Chapter 2).[18]

The proper recording of activities also helps to "cover" individual officers by demonstrating the authorisations they received to take particular action and documenting their role in a given case of cooperation. By way of example, UK intelligence officers are now required to record interviews that they conduct overseas with persons in detention.[19] This is intended to guard against accusations of (complicity in) abuse, as well as to provide a record of the information obtained. Finally, it should be noted that record keeping also helps services in building and maintaining accurate databases of information that may be pertinent to investigating and preventing threats to national security.

Maintaining a written record of actions and interactions is, however, challenging in an area of work that can be characterised by operational urgency and the prevalence of verbal, trust-based exchanges of information. Moreover, foreign partners may not have the same requirements for recording and providing grounds for particular requests or decisions, which makes it hard for services to compile a complete set of documentation. For example, services often receive perfunctory requests for information on a particular person; the request may not stipulate why the information is needed or what the person is suspected of doing. This can make it very difficult for the recipient service to make a proper assessment of whether or not its own guidelines permit it to provide the information.

With this in mind, services may need to demand that foreign partners normally submit their requests in writing, with appropriate provision for cases of operational urgency, and containing some basic information such as their grounds for suspicion (in requests for information on specific persons).[20]

The law often requires services to keep proper records of their activities. For instance, the principal law governing the Dutch intelligence services requires that the services record all transfers of personal data.[21] Recording transfers of information, regardless of the medium, is essential for documenting international intelligence cooperation. If information is provided orally in, for example, meetings between liaison officers, it is imperative that written reports or minutes are produced. By way of example, CSIS operational policy requires all employees to submit written reports following contact with a representative of a foreign service regardless of whether this takes place in Canada or abroad. These reports are considered to be crucial for managing, tracking, and monitoring CSIS' relationships with foreign partners.[22]

Additionally, it is good practice for all aspects of decisions relating to international intelligence cooperation to be fully documented.[23] This implies that services should record any requests received from or sent to foreign partners (outside fully regulated exchange arrangements), as well as a service's own responses to incoming requests from foreign partners. With regards to requests made to foreign partners, they should endeavour to ensure that they are properly motivated and contain as much information as possible. It is not only decisions that should be recorded but also how, by whom, and on what basis they were reached. For example, in the case of the aforementioned mentioned risk assessments, the person doing the assessment should record their evaluation of each criterion and the information used to reach particular conclusions.[24]

Recommendation:

There should be clear requirements on the recording of cooperation with foreign services. These should include requests made/received and information sent to/received from foreign services, as well as on internal decision making relating to international intelligence cooperation.

INTERNAL GUIDELINES

Services need comprehensive internal guidelines on how to handle all aforementioned aspects of cooperation with foreign services. Where appropriate such guidelines should be approved by the responsible minister, and they should be subject to the scrutiny of an external oversight body.

Box 6.4: Summary of issues to be included on services' internal guidelines on international intelligence cooperation

Services' internal guidelines on international intelligence cooperation should include but not be limited to:

- Criteria for risk assessments/due diligence relating to cooperation with foreign partners and specific guidance on how to conduct such assessments
- Requirements on record keeping relating to requests for information (incoming and outgoing), as well as on any information shared verbally
- Rules regarding caveats/conditions and reliability assessments to be placed on outgoing information
- Requirements to include provisos and reliability assessments when recording incoming information
- Guidance on information that is required from foreign services' before acceding to a request for assistance
- Procedures for obtaining authorisation for different forms of international intelligence cooperation
- Reporting requirements *vis-à-vis* the executive and external overseers
- Guidance on handling concerns about human rights abuses by foreign partners
- Guidance on conducting interviews abroad (including with persons who are in detention)
- In the context of joint SIGINT activities, how and by whom any selectors (search terms) proposed by a foreign partner will be evaluated and authorised.

PROCEDURES FOR INTELLIGENCE SERVICE PERSONNEL TO REPORT CONCERNS/WRONGDOING

Intelligence service personnel are generally the first people to become aware of problems relating to international intelligence cooperation. It is they who have regular contact with foreign partners, may observe their actions first hand, and may be best placed detect any concerns associated with specific instances of cooperation or a relationship, more generally.

Aside from the actions of cooperation partners, intelligence officers may also encounter information indicating wrongdoing in the practices or operations of their own service and/or the behaviour of particular colleagues. Concerns may relate to, for example, human rights, compliance with legal requirements pertaining to international intelligence cooperation, financial irregularities, the concealment of activities or information, improper record keeping, or the failure to cooperate with an oversight body.

Where an intelligence officer has information relating to possible wrongdoing by a foreign partner or their own service/colleagues, it is essential that there exist internal channels through which disclosures can be made, investigated and, if necessary, acted upon. It is equally important that intelligence officials are permitted to make disclosures to an external oversight body; this is especially important where concerns relate to actions

of senior managers or service policies/practices.[25] By raising concerns and disclosing information about possible wrongdoing to senior managers or, where appropriate, members of the executive and/or external oversight bodies, intelligence service personnel can fulfil and early warning function that can help to manage the risks associated with international intelligence cooperation.

Recommendations:

Intelligence services should be required by law to establish internal mechanisms through which their staff can disclose information or concerns relating to wrongdoing by a foreign partner or colleagues within their own service.

Intelligence service personnel should be permitted to make protected disclosures relating to international intelligence cooperation (or any other matters) to an external oversight body, which is required to investigate disclosures of information showing wrongdoing.

Governments should ensure that procedures and protections for intelligence service personnel wishing to disclose concerns comply with the minimum standards set out in the Global Principles on National Security and the Right to Information.

Intelligence service personnel can only fulfil this role if they are confident that they can disclose concerns without risking their careers or facing legal proceedings – i.e. they can make "protected" disclosures. The international principles in Box 6.5 below set out good practice regarding disclosures of wrongdoing by intelligence personnel.

6.3 Role of the executive

In any democratic polity, there are one or more ministers (members of the executive) responsible for intelligence services. Some countries, such as South Africa, have opted to have one minister who is responsible for the intelligence sector. More commonly, one or more intelligence services falls under broader ministerial portfolios such as defence, justice, home affairs, and foreign affairs. Executive control or oversight of international intelligence cooperation may also be exercised by a collective such as a national security council, as is the case in Croatia. The precise nature of ministerial control of and responsibility for intelligence services varies between states and depends on constitutional arrangements. This has implications for ministerial control of international intelligence cooperation because, for example, in some systems ministers are politically but not legally responsible for services' activities. Normally, both forms of responsibility apply.

THE IMPORTANCE OF EXECUTIVE INVOLVEMENT IN INTERNATIONAL INTELLIGENCE COOPERATION

There are a number of reasons for which ministers responsible for intelligence services need to exercise control over and oversight of international intelligence cooperation. First, ministers are politically and/or legally accountable for the activities of intelligence services and often required to defend their services, including their international intelligence

Box 6.5: Provisions on protected disclosures from the Global Principles on National Security and the Right to Information[26]

This box contains edited excerpts from the Global Principles on National Security and the Right to Information, which cover intelligence service personnel:

- The law should protect from retaliation […] public personnel who make disclosures of information showing wrongdoing, regardless of whether the information is classified or otherwise confidential, so long as, at the time of the disclosure: the person making the disclosure had reasonable grounds to believe that the information disclosed tends to show wrongdoing, that has occurred, is occurring, or is likely to occur, that falls within one of the categories [including]: criminal offenses; human rights violations; international humanitarian law violations; corruption; dangers to public health and safety; mismanagement or waste of resources; deliberate concealment of any matter falling into one of the above categories
- A person's motivation for making a protected disclosure is irrelevant except where the disclosure is proven to be knowingly untrue.
- Public personnel should be authorized to make protected disclosures to independent oversight bodies or to another body competent to investigate the matter without first having to make the disclosure internally.
- If a person makes a protected disclosure internally or to an independent oversight body, the body receiving the disclosure should be obliged to: investigate the alleged wrongdoing and take prompt measures with a view to resolving the matters in a legally-specified period of time [and] protect the identity of public personnel who seek to make confidential submissions […]
- A person who has made a disclosure, in accordance with [the principles] should not be subject to criminal or civil proceedings related to the disclosure of classified or otherwise confidential information.
- The law should prohibit retaliation against any person who has made, is suspected to have made, or may make a disclosure. Prohibited forms of retaliation include […]: administrative measures or punishments, physical or emotional harm or harassment; or threats of any of the above.

cooperation. In many countries, ministers may/should be held to account in parliament and by the public (and even in court) for the performance of services and for anything that goes seriously wrong. Illustrating this point, the Snowden revelations about cooperation in the context of bulk surveillance have caused considerable embarrassment and political damage to executives (see Chapter 3). Accordingly, it is in the interests of relevant members of the executive to take steps to ensure that services undertake international intelligence cooperation in a manner that is effective, lawful, and appropriate, as well as to ensure that they are informed about what is going on this domain. Recent disclosures relating to cooperation between the NSA and foreign intelligence services have highlighted that in some countries political executives have not been apprised of important aspects of international intelligence cooperation, and activities may have occurred without executive knowledge or authorisation.[27] To ensure that this doesn't happen ministers should lay down the policies under which intelligence activities are conducted, ensure they have sufficient knowledge of these activities, and, where appropriate, exercise some measure of control over certain types of activity (see the next section for further discussion).

Second, as was discussed in Chapters 2 and 3, international intelligence cooperation is closely linked to foreign relations. Given that relations with other states are an important prerogative of elected politicians, it is imperative that ministers are not only aware of services' cooperation with foreign partners, but they also assess foreign policy implications and provide appropriate guidance to services. Intelligence services have their own professional priorities and may not be best placed to assess the political foreign relations implications of their cooperation with foreign services. It is important that intelligence services are not left to conduct international intelligence cooperation in isolation from and (potentially) in contradiction with the state's foreign policy (see Chapter 3).

A division of ministerial responsibilities in some countries means that ministers responsible for foreign affairs are not responsible for intelligence services; services can fall under ministers of interior or defence. This is usually the case in states, such as Canada and the Netherlands, that do not have dedicated foreign intelligence services. Such arrangements can pose problems for ensuring alignment between international intelligence cooperation and foreign policy/relations, making it particularly important to ensure careful coordination between ministries responsible for services and ministries of foreign affairs. This applies both in the capital and in the field, where heads of mission/ambassadors should be kept apprised of services' liaison activities in the countries they are responsible for. Yet this remains important even in states where there are services under a foreign ministry because it is still necessary to ensure that services falling under other ministries conduct their international intelligence cooperation in accordance with foreign policy and consult in advance with the foreign ministry as appropriate (as is the requirement in the UK, for example).

Third, some aspects of international intelligence cooperation involve significant risks including the possible violation of human rights, damage to a state's reputation, political harm to an incumbent government, and legal risk for both states and individual intelligence officers (see Chapter 3). Because governments are responsible for the activities of state bodies and state agents, it is especially important that ministers exercise some control over activities that can have major consequences. Ministers may also be well placed to use their political influence to encourage foreign governments to, for example, adhere to assurances given regarding human rights compliance or to respect caveats on information sent to them.[28]

Finally, from the perspective of intelligence services, it is beneficial to have "political cover" for their international intelligence cooperation. Services may want the reassurance that particular relationships or activities have the approval of the executive because this helps to protect them from any political or legal fallout from international intelligence cooperation. This may take the form of ministerial authorisation for a particular operation or policy directives. A rare public example is the Canadian Ministerial Direction on Information Sharing, which was issued following conflicting public statements on CSIS' policy on the use of incoming information that may have been derived from torture.[29] CSIS would appear to have requested policy guidance from the minister. Services should be encouraged to involve ministers on controversial or high risk aspects of international intelligence cooperation.

SCOPE OF MINISTERIAL INVOLVEMENT

The extent of ministerial involvement in international intelligence cooperation varies significantly between states, over time and between individual ministers. Much depends on the breadth of his/her portfolio and/or individual ministers' level of interest in intelligence matters. Procedures for executive control and oversight of international intelligence cooperation need to take account of the fact that intelligence is often a small part of large ministerial portfolios and appropriately cleared officials should, therefore, assist ministers in this domain.[30] It is especially important that ministers equip themselves with knowledgeable officials in their departments who can advise on intelligence; they should not simply accept advice direct from their services. The fact that a minister has competing priorities and a lack of time is not a sustainable excuse for failing to remain apprised of developments services' international intelligence cooperation and ensuring that international intelligence cooperation is effective, appropriate and lawful.

Recommendations:

Ministers responsible for intelligence services should ensure that they have access to dedicated (non-intelligence service) staff who can advise them on decisions relating to the intelligence services.

Ministers should ensure that training on intelligence (including international intelligence cooperation) is given to the officials responsible for advising/assisting them in this area.

This subsection will discuss a number of ways in which ministers may be involved in international intelligence cooperation, and it will explain how such involvement can be beneficial. At the outset, it should be acknowledged that a balance needs to be struck between ensuring appropriate ministerial knowledge and stewardship of international intelligence cooperation (for the reasons outlined above) and preventing the politicisation of professional intelligence work. For example, it may not be desirable for a service to be directed to cooperate with a foreign partner because a minister wants to win favour on other matters with a foreign counterpart. What is required in terms of international intelligence cooperation should remain primarily a professional judgement call. Regardless of the precise functions of ministers in international intelligence cooperation, it is good practice for executive involvement to be regularised and not *ad hoc* – both parties need consistency in this regard. Some of the following functions are specific to international intelligence cooperation, but others are extensions of the general roles played by ministers responsible for intelligence services.

Reshaping and Re-Establishing Intelligence Relations

In countries in transition from authoritarian rule and/or emerging from a period of civil conflict, ministers may have a more prominent role to play in international intelligence cooperation. It will often be necessary to recalibrate intelligence relationships with foreign states, as well as to establish entirely new relationships. A good example is post-apartheid South Africa. The apartheid-era services had a very extensive network of liaison with foreign services, focussed on protecting the regime. Understandably, the new ANC-

led government did not share the same outlook or priorities for the intelligence sector. Given the sensitivities surrounding intelligence and the need to ensure that intelligence activities reflected the priorities of the new government, ministers played an active role in international intelligence cooperation. Several intelligence ministers worked closely with their foreign counterparts to development new intelligence relations.

Keeping Apprised of International Intelligence Cooperation Developments

Effective ministers will want to know sufficient information about what is going on in intelligence services within their portfolios to be able to discharge their ministerial accountability. Without such knowledge, ministers cannot take action, re-orientate, or curtail aspects of international intelligence cooperation, but they will, nevertheless, be held to account if something goes wrong. Recent revelations have raised the possibility that ministers in some states may not have had sufficient knowledge of some politically sensitive forms of international intelligence cooperation and intelligence activity, more generally.[31] This has underlined the need for ministers to require the services to keep them apprised of developments – this should happen notwithstanding any requirements for the ministers to authorise particular aspects of international intelligence cooperation.

It is good practice (and often a legal requirement) for intelligence services to hold regular discussions with the responsible minister or his/her representatives in order to inform him/her about ongoing work or particular concerns. Ministers can use these opportunities to ask follow-up questions on aspects of international intelligence cooperation. Ministerial staff can also proactively seek information and ensure that pertinent questions are asked of services, including about their foreign relationships. Services may be required to keep the responsible minister informed about their cooperation with foreign partners. For example, the Canadian Ministerial Direction on Information Sharing with Foreign Services imposes such a requirement on the director of CSIS[32] (see also Box 6.6 on a similar requirement in Norway).

Recommendation:

Ministers should require intelligence service heads to keep them apprised of relevant developments in their relationships with foreign services. They should use meetings/ briefings with service heads to enquire about international intelligence cooperation-related matters.

Ministerial Directives on International Intelligence Cooperation

Ministers should consider issuing to their services directives or policy statements on international intelligence cooperation that supplement (but must be consistent with) statutory provisions. Given the scarcity of statutory provisions on international intelligence cooperation, these directives can play a key role in establishing a sound legal and policy framework for international intelligence cooperation (see Chapter 5). Ministerial direction, dependent on circumstances, can usefully highlight specific issues such as interviewing detainees overseas (e.g. UK Consolidated Guidance, Box 6.7) or sharing personal data (e.g. Boxes 6.2 and 6.6 from Norway) of information with foreign intelligence services that have

poor human rights record (e.g. the Canadian Ministerial Direction on Information Sharing with Foreign Entities).

Box 6.6: Ministerial guidelines on the Norwegian Intelligence Service's disclosure of personal data to foreign services[33]

This edited extract is drawn from recently released Ministry of Defence guidelines. Personal data concerning Norwegian persons shall not be disclosed unless the following conditions are met:

- The disclosure takes place as part of the Intelligence Service's performance of its statutory tasks.
- The information in question is information that the Intelligence Service may lawfully hold.
- The disclosure is in Norway's interest.
- The disclosure of each item of information is deemed to be necessary in the case of personal data, or, in the case of sensitive personal data, strictly necessary, following a proportionality assessment in which safeguarding the national interests is weighed against the consequences for the person concerned.
- The disclosure is subject to a proviso whereby the information cannot be used as the basis for surveillance or covert information collection relating persons staying on Norwegian territory.
- The disclosure is deemed to be justifiable in light of the quality of the information, whom it concerns, who the recipient is, and the course of action the recipient is expected to take.
- The Intelligence Service shall provide the Ministry of Defence with an overview of all cases […in which it…] has disclosed personal data concerning Norwegian persons to foreign cooperating services.
- The authority to authorise such measures rests with the head of the Intelligence Service or whoever he/she authorises to make such decisions.

Many states have not developed ministerial directives on international intelligence cooperation; ministers have left it to services to develop internal regulations on international intelligence cooperation. That misses an opportunity to set down general parameters for important aspects of international intelligence cooperation and their expectations in terms of their own roles, those of service management and individual intelligence officers.

Recommendations:

Oversight bodies should verify whether there are ministerial guidelines in place that govern international intelligence cooperation.

Oversight bodies should identify areas of international intelligence cooperation decision making in which an intelligence service would benefit from ministerial direction.[34]

Services or the executive should consider publishing ministerial directives on international intelligence cooperation in order to promote discussion on such policies and to increase public confidence in the intelligence services.

Ministerial Approval of International Intelligence Cooperation

Although the nature and variety of intelligence work requires some flexibility regarding when ministers must be consulted/approve actions, it is important that directives are as clear as possible about which decisions are delegated to services and which are reserved to ministers. Clarity regarding the "level" of authorisation required for particular types of international intelligence cooperation and the risks whose presence triggers the need to consult ministers promotes consistency in decision-making. Such guidelines also assist with *ex post* review of and accountability for international intelligence cooperation. The *ad hoc* exercise of executive power in this domain is not helpful for services.

Most states require services to obtain ministerial approval before engaging in specific categories of operation, regardless of whether they involve international intelligence cooperation. For example, surveillance operations (involving the use of intrusive measures) in a service's own country may require ministerial authorisation, e.g. in the UK and the Netherlands, (sometimes in addition to judicial authorisation, e.g. Canada). Such requirements remain, regardless of whether such an operation is undertaken at the request of or in collaboration with a foreign partner. Similarly, services with mandates to work overseas, such as the UK's Secret Intelligence Service, normally require ministerial approval to conduct certain operations in foreign countries. This would include collaborative operations involving foreign services.

While it would be impractical and unnecessary for the executive to approve every instance of international intelligence cooperation, it is good practice for states to require that services seek ministerial approval before undertaking cooperation that poses particular risks. In the Netherlands, for example, specific instances of cooperation (e.g. granting assistance to foreign services and joint operations whereby foreign agents are active on Dutch territory) are undertaken under the direct responsibility of the minister.[35] The relevant minister must approve cooperation that involves "high-risk counterparts." The rationale given for requiring ministerial approval in these latter cases is that cooperation with such foreign services can have implications for Dutch foreign policy, in which human rights are an essential factor, or that the cooperation may have political consequences.[36] Information sharing relating to persons who are (or will be) in detention overseas can be high risk from a human rights perspective (see Chapter 3). Recognising this, the UK guidelines adopt a graduated approach to authorisation – requiring ministerial involvement in higher risk situations (see Box 6.7).

Box 6.7: Ministerial guidance to British intelligence officers on international intelligence cooperation where there is a risk of torture/CIDT[37]

This is an edited extract from ministerial guidance issued to intelligence officers on interviewing detainees overseas and the passing and receipt of intelligence relating to detainees held by foreign services.

	Situation	Action
Level of risk of torture and/or cruel inhuman and degrading treatment	If you know or believe torture will take place	1. You must not proceed and Ministers will need to be informed 2. You should raise concerns with liaison or detaining authority to try and prevent torture occurring unless in doing so you might make the situation worse.
	If you believe there is a risk of torture or a serious risk of CIDT.	1. You must consult senior personnel. You must not proceed unless either: • Senior personnel and legal advisers conclude that there is no serious risk of torture or CIDT, or; • You are able to effectively mitigate the risk of mistreatment to below the threshold of a serious risk through reliable caveats or assurances 2. If neither of the two preceding approaches apply, ministers must be consulted. Ministers will need to be provided with: • Full details, including the likelihood of torture or CIDT occurring, risks of inaction and causality of UK involvement Ministers will consider whether: • It is possible to mitigate the risk of torture or CIDT occurring through requesting and evaluating assurances on detainee treatment; • Caveats placed on information/questions would be respected by the detaining liaison partner; • UK involvement in the case, in whatever form, would increase or decrease the likelihood of torture or CIDT occurring. Consulting Ministers does not imply that action will be authorised but it enables Ministers to look at the full complexities of the case and its legality
	In circumstances where you judge there is a lower than serious risk of CIDT taking place and standards of arrest and detention are lawful	You may proceed, keeping the situation under review.

Even when ministerial approval is not required under any regulations, if services have any concerns, it is good practice for them to inform and seek approval from the relevant minister before engaging in cooperation. The Canadian Ministerial Directive on Information Sharing with Foreign Entities gives the director of CSIS the option of deferring decisions on information (in high-risk cases) to the minister.[38]

Recommendation:

Ministerial or intelligence service guidelines should make clear which types of international intelligence cooperation-related decisions require consultation with and/or the approval of ministers. Overseers should evaluate whether such guidelines require appropriate decisions to be referred to ministers and whether the guidelines are followed in practice.

Ministerial Approval of Cooperation Agreements with Foreign Services

International intelligence cooperation is often based on bi/multilateral agreements between services and sometimes agreements between governments, such as defence treaties (see Chapter 4). Some states require, as a matter of law and/or customary practice, that ministers approve the adoption of service-service agreements. This is the case in the US, where the Director of National Intelligence must approve any new formal SIGINT relationships with foreign services.[39] Canada's CSIS may "with the approval of the Minister after consultation by the Minister with the Minister of Foreign Affairs, enter into an arrangement or otherwise cooperate with the government of a foreign state or an institution thereof or an international organization."[40] Similarly in Croatia, "the establishment and the suspension of the cooperation with each foreign service is approved by the National Security Council on the basis of the recommendations of the directors of the security intelligence agencies."[41] This control function is intended to ensure that services cannot engage in substantive cooperation with a foreign partner without executive approval, and it enables the executive to ensure that agreements include appropriate safeguards. In considering whether or not to approve a new agreement, ministers should seek legal advice and discuss the foreign policy implications with relevant colleagues.

Recommendation:

The law should require that the executive approves any new or significantly-amended agreement or memorandum of understanding between an intelligence service and a foreign entity.

Endnotes

1. These guidelines are contained in an internal manual drafted by the service's Foreign Relations Department. While they remain classified, the CTIVD provided an in-depth assessment of the guidelines in: The Netherlands, *Review Committee for the Intelligence and Security Services* (CTIVD), Review report on the cooperation of GISS with foreign intelligence and/or security services, no. 22A, (The Hague, 2009), 6-14.
2. Canada, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (Arar Inquiry), *Report of the Events Relating to Maher Arar: Analysis and Recommendations*, (Ottawa: Public Works and Government Services Canada, 2006), 347.
3. CTIVD, *Review report on the cooperation of GISS with foreign intelligence and/or security services*, 44.
4. Arar Inquiry, *Report of the Events Relating to Maher Arar: Analysis and Recommendations*, 348. For discussion, see: Kent Roach, "Overseeing Information Sharing," in *Overseeing Intelligence Services: A Toolkit*, ed., Hans Born and Aidan Wills, (Geneva: DCAF, 2012).
5. Australia, Inspector-General of Intelligence and Security, *Inquiry into the actions of Australian government agencies in relation to the arrest and detention overseas of Mr Mamdouh Habib from 2001-2005* (hereafter: the Habib Inquiry), (Canberra: December 2011), 111-112.
6. Arar Inquiry, *Report of the Events Relating to Maher Arar*, 342.
7. Ibid., 13, 110-114, 119-123.
8. Roach, "Overseeing Information Sharing," 136.
9. Canada, Frank Iacobucci, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin*, 69-71.
10. Norway, EOS Committee, *The EOS Committee's oversight of information exchange with cooperating foreign services*, unpublished memo. See also: Norway, EOS Committee, *Annual Report*, 2005.
11. Australia, Inspector-General of Intelligence and Security, *Habib Inquiry*.
12. United Kingdom, *Report of the Detainee Inquiry*, December 2013, 23-24.
13. Ibid., 25.
14. Ibid., 45-68.
15. Canada, *Ministerial Direction to the Canadian Security Intelligence Service: Information Sharing With Foreign Entities*, 28 July 2011, Section 4.
16. CTIVD, *Review report on the cooperation of GISS with foreign intelligence and/or security services*, 22.
17. United Kingdom, *Report of the Detainee Inquiry, December 2013, 29; See also: Charkaoui v. Canada (Citizenship and Immigration)* 2008, 2 SCR 326, para 30-46.
18. Kate Connolly, "German secret service BND reduces cooperation with NSA," *The Guardian*, 7 May 2015.
19. United Kingdom, *Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees,* (London: Cabinet Office, July 2010), para 22.
20. Norway, EOS Committee, *Annual Report 2005*; The Netherlands, Review Committee for the Intelligence and Security Services (CTIVD), *Review report on the cooperation of GISS with foreign intelligence and/or security services*, 29.
21. The Netherlands, *Intelligence and Security Services Act 2002*, Article 42.
22. Canada, Security Intelligence Review Committee, *CSIS Liaison with Foreign Agencies – Review of the SLO Post (SIRC Study 2005-02)*, 21 March 2006, 19-21. See also: Netherlands, Review Committee for the Intelligence and Security Services (CTIVD), *Review report on the cooperation of GISS with foreign intelligence and/or security services*, 23.
23. Australia, Inspector-General of Intelligence and Security, *Habib Inquiry*, 114.
24. CTIVD, *Review report on the cooperation of GISS with foreign intelligence and/or security services*, 26; Arar Inquiry, *Report of the Events Relating to Maher Arar: Analysis and Recommendations*, 347-348.
25. See further: Benjamin S Buckland and Aidan Wills, "Blowing in the Wind? Whistleblowing in the Security Sector," *OSF-JI Working Paper*, 2012.
26. *Global Principles on National Security and the Right to Information (Tshwane Principles)*, adopted at Tshwane, South Africa on 12 June 2013, principles 37-39, 41.
27. Glenn Greenwald, "Foreign Officials in the Dark About Their Own Spy Agencies' Cooperation With NSA," *The Intercept*, March 13, 2014.
28. United Kingdom, *Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees*.

29. "CSIS defies orders on torture," *Toronto Star*, 1 April 2009; "CSIS official does about-face on torture testimony," *CTV News*, 2 April; CSIS Memo to Minister of Public Safety, 15 January 2008.
30. Cyrille Fijnaut, Het toezicht op de inlichtingen- en veiligheidsdiensten: de noodzaak van krachtiger samenspel De vertrekpunten en uitkomsten van een gespreksronde [The review of intelligence and security services: The necessity of stronger coordination (The results of a consultation)], (CTIVD: The Hague, 2012).
31. For an overview, see: Glenn Greenwald, "Foreign Officials In the Dark About Their Own Spy Agencies' Cooperation with NSA," *The Intercept*, 13 March 2014; *Der Spiegel*, "Spying Close to Home: German Intelligence Under Fire for NSA Cooperation," 24 April 2015; Michel Sauga et al., "'Secrets Must Remain Secret': German Intelligence Coordinator on NSA and Media Leaks," *Der Spiegel*, 14 August 2015.
32. Canada, *Ministerial Direction to the Canadian Security Intelligence Service: Information Sharing With Foreign Entities*, 28 July 2011, Section 3.
33. Norway, *Supplementary provisions concerning the Norwegian Intelligence Services' collection of information relating to Norwegian persons abroad and the disclosure of personal data to cooperating foreign services*, Adopted by the Ministry of Defence on 24 June 2013 pursuant to Section 17 of the Instruction for the Norwegian Intelligence Service.
34. See for example: The Netherlands, Review Committee for the Intelligence and Security Services, *Review Report on the processing of telecommunications data by GISS and DISS*, CTIVD NO. 38, 5 February 2014, 38; Canada, Security Intelligence Review Committee, *CSIS's Role in the Matter of Omar Khadr*, SIRC Study 2008-05.
35. CTIVD, *Review report on the cooperation of GISS with foreign intelligence and/or security services*, 29, 33.
36. Ibid., 7, 28-29.
37. United Kingdom, *Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees*, Cabinet Office, July 2010, 4-5.
38. Canada, *Ministerial Direction to the Canadian Security Intelligence Service: Information Sharing With Foreign Entities*, 28 July 2011, Section 4.
39. US, National Security Agency, *What Are We After with Our Third Party Relationships? — And What Do They Want from Us, Generally Speaking? The Intercept*, 13 March 2014.
40. Canada, *Canadian Security Intelligence Service Act 1989*, c23, s17(1)(b).
41. Croatia, *Act on the Security System of the Republic of Croatia 2006*, Article 59.

7

External Oversight of International Intelligence Cooperation

7.1 Introduction

This chapter will focus on the role of standing or permanent intelligence oversight bodies that are independent of and external to both the intelligence services and the executive. Such bodies include parliamentary committees, whose remit covers intelligence services (this may include dedicated oversight intelligence committees, defence, interior/home affairs and human rights committees); expert, non-parliamentary expert oversight bodies (including committees and single officeholders); and some independent regulatory bodies whose jurisdiction includes the intelligence sector, e.g., supreme audit institutions. This chapter will not address the important role that *ad hoc* commissions of inquiry have played in examining allegations of wrongdoing associated with international intelligence cooperation (some of these examples are discussed in Chapter 8). Equally, we will not consider the important role that has been played by international institutions in investigating and reporting on various aspects of international intelligence cooperation, including the Parliamentary Assembly of the Council of Europe, the European Parliament, and the UN special mandate holders.[1]

External oversight of international intelligence cooperation (and intelligence services, more generally) serves several general purposes. These objectives are not normally accomplished by any single external oversight body but by a system of external oversight

comprising the institutions mentioned above. A first objective of external oversight of international intelligence cooperation is to help to ensure/improve the effectiveness and utility of international intelligence cooperation by examining how far cooperation with foreign services contributes to national security and other relevant interests. Second, external oversight can assess whether intelligence service policies and activities have complied or will comply with applicable law. Third, and related to the first two categories, external oversight of international intelligence cooperation can help services and the executive to improve policies and practices.[2] Finally, external oversight can contribute to promoting public assurance and understanding about their services' cooperation with foreign bodies, particularly if they are regarded as being independent and above party politics. Oversight bodies can achieve this by making public their findings and reports on issues connected to international intelligence cooperation (see below for examples). This is especially significant at a time when international intelligence cooperation has given rise to public concern.

Very few statutes regulating external oversight of intelligence explicitly mandate scrutiny of international intelligence cooperation (see Chapter 5). Canada is a notable exception as legislation explicitly provides that one of the functions of the Security Intelligence Review Committee (SIRC) is to review arrangements entered into and cooperation with foreign states.[3] For most oversight bodies, international intelligence cooperation remains a recent subject of interest, as cooperation with foreign entities has become an increasingly prominent feature of services' work. Revelations about the human rights implications of international intelligence cooperation in the context of counterterrorism have compelled some oversight bodies to examine aspects of international intelligence cooperation (see Boxes 7.4-7.6 for examples). In most countries, however, international intelligence cooperation remains an under-scrutinised area of services' work; oversight bodies have yet to examine in a systematic or regular manner their services' cooperation with foreign partners. Various factors may explain this, including: the mandates of oversight bodies, sensitivities surrounding international intelligence cooperation, difficulties in acquiring necessary information, competing priorities, and a lack of resources. However, as this policy guide has made clear, overseers cannot afford to neglect this growing dimension of intelligence activity.

Recommendation:

Consideration should be given to providing external oversight bodies an explicit legal mandate to scrutinise international intelligence cooperation. Regardless of whether their mandate refers to international intelligence cooperation, oversight bodies should (if they have not done so already) monitor their services' cooperation with foreign partners.

At the outset, it is important to recall that legislation mandates standing oversight bodies to monitor intelligence services and/or associated executive entities in only their own state. They are responsible for evaluating their country's intelligence services' actions regarding, for example, information sharing, joint operations, and handling requests received from foreign partners. Overseers conduct such assessments and hold their

country's officials to account in accordance with national law. It is not, however, the role of oversight bodies to scrutinise the actions or policies of foreign services and their governments per se. To illustrate this, overseers might examine whether a decision by their service to send information to a foreign partner was taken in accordance with policy and the law. Beyond looking at publicly available information/reports, they would not, however, be in a position assess whether a request submitted by a foreign service was lawful or properly motivated, or how information sent to that service was used. Since international intelligence cooperation involves at least two or more countries, the issue of multiple jurisdictions poses formidable challenges for oversight bodies to scrutinise and pass judgement on the actions of foreign entities.

The chapter begins by discussing aspects of international intelligence cooperation that external oversight bodies should examine, it then considers the approaches and methods that overseers use to scrutinise international intelligence cooperation. The following section addresses the critical issue of access to international intelligence cooperation-related information by external overseers. The next section considers the important role that overseers can play in improving transparency in this area of intelligence work. The chapter will then examine possible international cooperation between external oversight bodies as means for strengthening oversight of international intelligence cooperation.

7.2 Aspects of international intelligence cooperation requiring external oversight

Earlier chapters in this guide set out a framework for the external oversight of international intelligence cooperation. Chapter 3 highlighted the benefits and risks associated with international intelligence cooperation; the issues discussed may assist overseers in determining which aspects of international intelligence cooperation to prioritise for scrutiny. Chapter 6's overview of intelligence services' internal control mechanisms provides additional entry points for external overseers – reviewing the effectiveness/adequacy of these internal mechanisms is especially important because services are best placed to ensure that international intelligence cooperation is lawful, appropriate, and effective. Given that external oversight also focuses on decisions of the executive, the discussion of the role of the executive in Chapter 6 provides further guidance on what external overseers should examine in this regard.

The scope and focus of external oversight of international intelligence cooperation will depend on an oversight body's mandate, powers, and resources, as well as their services' foreign relationships. Legal mandates of oversight bodies will influence the features of international intelligence cooperation that may be examined, as well as the criteria according to which activities or policies are assessed. Few, if any, oversight bodies have the resources to examine all of these issues across all periods of time. International intelligence cooperation is only one aspect of the work of services that overseers have to examine. They must, therefore, prioritise particular aspects of international intelligence cooperation. In deciding which aspects of international intelligence cooperation upon which to focus, overseers may consider factors such as: findings of previous reviews/

investigations; concerns raised in the media or by NGOs; complaints received from members of the public (if they have a complaints handling function); concerns raised by members of the services; the amount of resources services allocate to particular programmes; and the work of the oversight bodies in comparable states.

This section will provide an overview of some of the aspects of international intelligence cooperation that overseers may wish to scrutinise.[4] The following "subjects" of oversight will be discussed:

- Effectiveness of cooperation with foreign entities
- The legal and (operational) policy framework for international intelligence cooperation
- High-risk relationships
- Risk assessment processes
- Personal data exchanges and their human rights implications
- Caveats and assurances relating to information sent to foreign services
- Reporting and records keeping
- Joint operations
- Provision of training and equipment to foreign services
- Services' training of their own staff
- Financial transactions relating to international intelligence cooperation
- Role of the executive in international intelligence cooperation

These are not mutually exclusive categories, and there may be a number of different approaches to scrutinising the same facets of international intelligence cooperation. As was noted above, there are a variety of different external oversight bodies that should be involved in scrutinising international intelligence cooperation. Some of these bodies necessarily focus on aspects of international intelligence cooperation that are germane to their specific mandates. Most obviously, privacy or data protection commissioners only examine policies and practices relating to exchanges of personal data. Because the types of oversight bodies that exist and the division of labour between them vary from state to state, this guide will not prescribe international intelligence cooperation oversight roles for specific types of oversight body. It will, nevertheless, indicate where certain types of oversight body are more likely to scrutinise particular dimensions of international intelligence cooperation.

EFFECTIVENESS OF INTERNATIONAL INTELLIGENCE COOPERATION

A primary role of external overseers is to hold the executive to account for the overall effectiveness of the services, and that should include their cooperation with foreign states. This is a task that is most commonly performed by parliamentary intelligence oversight committees, in the context of questioning ministers about intelligence budgets, annual intelligence priorities, and activity reports, as well as when there has been an intelligence failure. Supreme audit institutions may also play a role in this regard; a discussion of their role is beyond the scope of this book.[5]

External scrutiny of international intelligence cooperation should go beyond looking at matters of legality and propriety. As Chapter 3 demonstrated, cooperation with foreign services is essential for enabling services to contribute to protecting national security and public safety. Overseers may wish to test, for example, whether intelligence services are engaging in sufficient cooperation with the right foreign partners and whether they are maximising possible benefits from cooperation. An external overseer may want to assess whether a given relationship with a foreign partner is beneficial in terms of acquiring pertinent information or other resources; represents value for the resources invested; creates a risk of over-reliance/dependency that could harm national security; and/or has a sufficient degree of *quid pro quo*. Such assessments are inevitably policy-laden and will be more complex than assessments of lawfulness, and there is no single framework against which to assess international intelligence cooperation effectiveness and benefits from international intelligence cooperation, which, like any intelligence reporting, may be fragmentary and uncertain with an impact that is difficult to gauge.

The primary responsibility for monitoring such matters in detail rests with the executive, but it may also be helpful for an external body to oversee the effectiveness of international intelligence cooperation taken as a whole. Scrutiny of the effectiveness of cooperation requires an oversight body that has a mandate that goes beyond examining lawfulness. Parliamentary oversight committees may be well placed to examine these matters at a general level. They are well placed to take steps to ensure that services have sufficient budgets and legal powers to undertake effective international intelligence cooperation. Supreme audit institutions (SAIs) could provide particular expertise in evaluating value-for-money and performance of some forms of cooperation relative to resources invested. Expert intelligence oversight bodies may also play a role. Belgium's Standing Intelligence Agencies Review Committee (Committee I), a non-parliamentary expert body, has touched on the services' exchange information in the context of investigations into how the services tackle particular threats. One example was an investigation into the Belgian services' monitoring of the proliferation of non-conventional weapons. While the public report does not demonstrate an in-depth assessment of how effectively international intelligence cooperation contributes to this work, this is an example of an entry point that overseers might use to assess the effectiveness of cooperation.[6]

LEGAL AND OPERATIONAL POLICY FRAMEWORK

Evaluating the legal framework and operational policy that governs an intelligence service's cooperation with foreign entities is an essential component of oversight of international intelligence cooperation. In particular, external oversight bodies may wish to examine whether ministerial guidelines, internal regulations, and a service's operational policy comply with relevant national and international human rights law.

An obvious starting point for external overseers is to examine any primary and secondary legislation governing international intelligence cooperation. However, given that most countries' legislation provides little detail on international intelligence cooperation, it is also necessary to examine ministerial directives and internal guidelines regulating international intelligence cooperation. Memoranda of understanding or cooperation

agreements with foreign entities may also be an important component of the legal framework for cooperation and should be scrutinised by overseers.[7] External oversight bodies should pay particularly close attention to services' operational policies because they generally provide the most detail on how, why, and according to what procedures staff can engage in cooperation with foreign entities (see examples in Chapter 6).

Scrutiny of any aspect of a service's cooperation with foreign entities is likely to require an assessment of the regulations and operational policies that govern such relationships, both in cases where an oversight body is, for example, examining specific cases/incidents relating to cooperation (e.g., the Australian IGIS' examination of the Habib case, see Box 7.6 below) and in examining a service's risk management processes. In addition to the appropriateness of the legal and policy framework for cooperation, overseers will need to examine its implementation in practice against that framework.

HIGH-RISK RELATIONSHIPS

External overseers may wish to focus on scrutinising services' "high-risk" international intelligence cooperation relationships. This is cooperation with foreign entities where the risks of, for example, human rights violations, reputational damage, and inconsistencies with foreign policy are considered to be high (see Chapters 3 and 4). Focusing on these relationships may be helpful in view of the time and resource limitations faced by all oversight bodies. It is, nevertheless, important that overseers do not ignore cooperation with services from democratic states, both because these are likely to be the dominant relationships and because experience over the last decade has demonstrated that services underpinned by the law and subject to external oversight can still engage in practices that create political and legal risk for the cooperating state (see Chapter 3).

Oversight of specific high-risk relationships might focus on the terms of any cooperation agreement or MoU in place with a given partner, the services' risks assessments of the partner, any personal data sharing, the use of caveats, and the seeking of assurances regarding shared information.

RISK ASSESSMENT PROCESSES

Chapter 6 highlighted the critical importance of services conducting risk assessments or due diligence processes before entering into cooperation with foreign services. Risk assessments include evaluating, for instance, foreign services' reliability in handling information, its human rights record, and its legal and oversight framework. Accordingly, overseers should pay considerable attention to the way that services conduct risk assessments and how different risks and benefits are weighed. Oversight bodies may examine the criteria services use for these assessments, what information they draw upon, the reasoning adopted to support assessments in specific cases, and whether or not assessments of foreign services comport with the conclusions of other bodies such as foreign ministries and major NGOs. The Dutch CTIVD, a non-parliamentary expert oversight body, undertook a detailed assessment of how the AIVD conducts such assessments in the context of its extensive thematic investigations into the service's cooperation with foreign

partners. The Committee looked not only at assessments of risk but also of potential benefits from cooperation.[8]

PERSONAL DATA EXCHANGES AND THEIR HUMAN RIGHTS IMPLICATIONS

Oversight of personal data exchanges with foreign entities is most likely to be a task for expert non-parliamentary oversight bodies and/or privacy and information commissioners. This is because it demands a depth of scrutiny that parliamentary committees do not normally have the time, expertise, or resources to conduct.

In view of the human rights consequences of sharing personal data, external oversight of the policies and processes for exchanging data with foreign entities, as well as specific instances of personal data sharing is recommended. Given the volume of personal data that is shared and limited resources available to overseers, they may consider focusing on personal data sharing policies and processes while examining specific cases in the context of relationships or operations that are considered to be particularly high risk.

Regarding specific cases of personal data sharing, overseers should examine factors such as whether the data exchange complied with applicable laws (including on legitimate purposes for personal data sharing, proportionality requirements and any required level of suspicion), was properly recorded (see below), appropriate caveats were attached to the information, and/or any assurances were sought from a foreign service (see below). If personal data is transferred on the basis of a request from a foreign partner, overseers can examine whether it was reasonable to send the information in view of the scope and preciseness of the request.

By way of example, this has been a focus of Norwegian EOS Committee's oversight of international intelligence cooperation. The Committee regularly examines personal data exchanges to assess who data was sent to, whether disclosures were made for lawful purposes, and whether they are proportionate from a human rights perspective. Box 7.1 highlights some of the questions that the Committee has put to the domestic intelligence service regarding its sharing of information with foreign entities.[9] Oversight of personal data exchanges normally focuses on outgoing information, i.e. data sent by the relevant Norwegian service.

Box 7.1: Examples of questions Norway's EOS Committee has addressed to the Police Security Service (PST) as part of scrutiny of the Service's international intelligence cooperation

- What control measures does the PST carry out before disclosing information (to a foreign entity) in order to ensure that the conditions under Section 4.1 of the Act are met?
  These conditions are:
  - Information can be shared in order to avert or prevent criminal offences or if it is necessary in order to verfiy information
  - Before information is shared, there must be an assessment of the proportionality between the purposes of sharing the information and the consequences for individuals.
- Do any special conditions apply to the disclosure of unverified information?
- What factors are included in the assessment of whether the consequences for individuals are proportionate to the purposes of the disclosure of information to a foreign entity?
- Can examples be given of assessments made in connection with requests for disclosure of biometric data?
- Does the PST make written assessments in connection with requests for disclosure of biometric data?
- Where and how does the PST record an overview of information disclosed by the PST? And do such overviews show why information has been disclosed?

The scrutiny of processes for handling *incoming information* implies a different focus for overseers. They may wish to examine how requests for information are normally formulated and the level at which they are signed off. In this regard, an assessment might focus on how a request is made, the type of information likely to be requested, what the valid reasons were for requesting it including what the service knew about the person and their location, whether it has already targeted the persons concerned, and any implications that making the request might have for persons concerned. Overseers will wish to satisfy themselves that there is no risk that services can use international intelligence cooperation to circumvent legal safeguards that apply to their own information collection. Overseers may also examine how services register incoming personal data, including and whether they attach information about its origin and any concerns about reliability.

Recommendation:

There should be at least one external oversight body that is empowered to scrutinise the policies the practices relating to both the outgoing and incoming sharing of personal data with foreign entities.

CAVEATS AND ASSURANCES RELATING TO INFORMATION SENT TO FOREIGN SERVICES

Caveats are conditions attached to information sent to foreign services, imposing restrictions on the use of the information. As was discussed in Chapter 6, they can help to ensure that information is not used in a way that may compromise its confidentiality or as a basis for violating human rights. In addition to caveats, services may request written assurances from foreign partners regarding the use of outgoing information. External overseers can examine the policies for the use of caveats and assurances relating to outgoing information. More specifically, oversight bodies can check whether caveats are sufficiently clear and comprehensive, and whether services are satisfied that they are fully understood by a foreign partner. It may be difficult for services to assess compliance with caveats and assurances, but overseers can, nevertheless, enquire about any such assessments.

REPORTING AND RECORDS KEEPING

The importance of information management and record-keeping in relation to international intelligence cooperation was discussed in Chapter 6. External overseers (and courts) cannot properly review actions and decisions if they have not been documented or if records are incomplete. For this reason (and for the purposes of services' own efficiency) record keeping is an area that overseers can usefully examine (see Chapter 5, Box 5.4). For example, annually, the Australian IGIS checks the services' recording of information exchanges, including the documenting of decisions about information exchanges. Canada's SIRC frequently examines this subject in the context of its scrutiny of CSIS's "security liaison posts;" that is, stations overseas through which information is shared with foreign services. Among other things, the SIRC assesses whether or not contact with representatives is properly recorded and reported back to headquarters.[10]

How intelligence services document decisions on international intelligence cooperation and their exchanges with foreign services has implications for the oversight of other aspects of international intelligence cooperation discussed here. By way of example, overseers cannot properly evaluate risk management processes if there is no record of who conducted a risk assessment and what information they used. Similarly, they cannot assess whether personal data sharing is done in compliance with the law and policy if there are incomplete records of transfers and the bases for them. This can undermine the oversight of international intelligence cooperation regardless of the access-to-information powers available to an oversight body.

COVERT OPERATIONAL COOPERATION

Covert operational cooperation or joint operations are one of the most sensitive and high-risk areas of international intelligence cooperation from the perspective of human rights and the rule of law (see Chapter 3). They are also an area of international intelligence cooperation that may be unlikely to be revealed to overseers during the course of routine oversight. As discussed in Chapter 2, covert operational cooperation takes many different

forms and includes joint surveillance activities and various forms of covert action taken to, for example, disrupt threats.

Overseers will need to make enquiries about covert operation cooperation and examine whether any surveillance or other actions taken by their own services, in the context of joint operations, complied with the applicable national legislation, as well as the state's international human rights obligations. This includes questions of whether or not measures were properly authorised, whether services complied with any warrant, and how services recorded and used the information collected. In the context of joint surveillance operations, scrutinising such matters is an extension of the role that many oversight bodies already play in examining the authorisation and use of surveillance measures as part of their non-international intelligence cooperation focused work. Finally, overseers should also evaluate what their services have authorised foreign services to do on their territory and ensure that this complies with the law.

PROVISION OF TRAINING AND EQUIPMENT TO FOREIGN SERVICES

Some intelligence services provide equipment and training to foreign intelligence services (see Chapter 2 for examples). The provision of such support can help to develop effective partners in other regions of the world. However, in some situations, it may also serve to enable foreign services to, for example, monitor political opponents and NGOs or to track down persons who are later subject to unlawful detention. In view of this, oversight bodies should examine what training or equipment is being provided to foreign services and whether this is consistent with the state's foreign and development policy. Overseers may also examine whether appropriate human rights training has been provided alongside operational training on matters such as surveillance or interrogation.

Oversight bodies in states whose services are the recipients of training and equipment (or other resources) from foreign partners should also scrutinise such "aid." Notably, overseers may wish to examine whether equipment provided to their services by foreign partners can be used under domestic law. It may also be relevant for overseers to look at what, if anything, has been provided by their services in exchange for assistance provided by a foreign partner. Where incoming support includes the provision of financial resources, relevant oversight bodies should ensure that any money is properly accounted for, and its use is subject to the same level of scrutiny as money allocated from the national budget.

SERVICES' TRAINING OF THEIR OWN STAFF

External oversight bodies can examine how services train their staff on compliance with laws and policies relevant to international intelligence cooperation. The attitude and knowledge of individual intelligence officers is a critical factor in determining whether or not cooperation with foreign partners is both beneficial to the service and done in accordance with the law. Oversight bodies can examine training curricula to ensure that relevant laws, policies, and issues of concern are included in training programmes. For example, the Australian IGIS has recommended changes to training courses and has recently gone further by contributing to the delivery of training to intelligence service

staff. The incumbent IGIS has addressed conferences of Australian Security Intelligence Organisation overseas-based liaison staff, in order to raise awareness about the importance of guidelines on exchanging information and the human rights implications thereof.[11] This is an excellent example of how overseers can play a direct role in improving the performance of intelligence services. Once again, this is most likely to be a task for members and staff of non-parliamentary expert oversight bodies, who deal with intelligence issues as a (near) full-time role.

FINANCIAL TRANSACTIONS RELATING TO INTERNATIONAL INTELLIGENCE COOPERATION

External auditors scrutinise intelligence service finances *ex post*, i.e. they look at annual budgets allocated to intelligence services and, later, at how such budgets were implemented.[12] Scrutinising money allocated to, expended on, or derived from intelligence activities helps to ensure financial propriety and compliance with the law. External oversight of intelligence service finances is also as an entry point for examining the efficiency and effectiveness of particular programmes or activities, including international intelligence cooperation. External financial oversight may include an examination of finances associated with particular forms of international intelligence cooperation (e.g., money spent on technological cooperation, joint surveillance infrastructure, or support to the development of a foreign service) or international intelligence cooperation in the context of particular geographical regions.

Overseers of services that play a role in building the capacity of foreign services may wish to pay particularly close attention to the allocation of funds (and other resources), rules surrounding their use, and any reporting requirements to ensure funds are not being used in a manner that is inconsistent with the donor state's (service's) laws and values. Overseers need to be especially watchful of whether the authorisation processes for provision of resources to foreign services take foreign policy into account. It is not only the overseers of "donor" intelligence services that need to focus on the financial aspects of international intelligence cooperation. The overseers of intelligence services that receive assistance from foreign entities should also pay attention to how incoming resources (including monetary transfers and equipment) are allocated and used. They can also ensure that regulations exist requiring that incoming resources are recorded and subject to audit by an external overseer.

> Recommendation:
>
> Overseers responsible for scrutinising intelligence budgets should examine the allocation and use of financial resources for international intelligence cooperation, including for providing equipment and training to foreign entities and joint surveillance infrastructure.

Parliamentary committees (including those responsible intelligence, budgets, and public accounts) may be able to use their budget amendment, approval, and/or discharge powers to require changes in programmes. If parliamentarians have concerns about particular activities or programmes relating to international intelligence cooperation, they may be

able to exercise such powers to require changes in international intelligence cooperation policies and practices. For such powers to be exercised effectively, it is important that parliamentary committees coordinate with SAIs (parliament should also ensure that SAIs have the necessary powers and resources). Such coordination helps to ensure that SAI audits cover relevant aspects of international intelligence cooperation and that SAI findings/recommendations are implemented in future budgets and financial policies.

ROLE OF THE EXECUTIVE IN INTERNATIONAL INTELLIGENCE COOPERATION

External oversight of international intelligence cooperation should take account of the role and responsibilities of the executive in this area. Depending on their mandate, oversight bodies may review the following aspects of executive involvement in international intelligence cooperation: ministerial authorisation of international intelligence cooperation-related activities; ministerial directions on international intelligence cooperation (including an assessment of whether they comply with the law); ministers' to remain apprised of developments in services' cooperation with foreign entities; ministerial knowledge of activities that have generated concern and/or complaints; and coordination of international intelligence cooperation across relevant ministries, including actions to ensure that international intelligence cooperation is consistent with foreign policy. Where relevant, external oversight bodies should seek to encourage consistent and predictable executive involvement in international intelligence cooperation. Overseers can also encourage ministers to establish guidelines on which international intelligence cooperation decisions and/or operations require ministerial consultation or approval.

Recommendations:

An external oversight body should evaluate executive involvement in international intelligence cooperation to assess whether it is sufficient and consistent.

External overseers should evaluate the adequacy of processes used to keep the executive informed about intelligence service cooperation with foreign entities.

External overseers should examine whether there are ministerial directives relating to international intelligence cooperation, ensure that any directives are consistent with the legislation, and highlight areas in which further ministerial guidance may be beneficial.

Oversight of the role of the executive in international intelligence cooperation is an area in which relevant parliamentary committees (as opposed to expert non-parliamentary oversight bodies) normally play the pre-eminent role. Made up of politicians, these committees are likely to have the requisite political expertise and authority to engage with the executive on these issues. By regularly questioning ministers about their stewardship of international intelligence cooperation, parliamentary oversight committees can help to ensure that ministers fulfil their responsibilities in this field. If ministers are aware that they will be questioned on and held to account for the services' cooperation with foreign entities, they are far more likely to pay close attention to international intelligence cooperation and (where applicable) authorise some aspects of international intelligence cooperation.

7.3 Approaches and methods for external oversight of international intelligence cooperation

Overseers may scrutinise the aforementioned aspects of international intelligence cooperation in many different contexts including through case-specific investigations, thematic investigations, and periodic inspections/assessments. This section begins by examining different contexts in which oversight bodies scrutinise international intelligence cooperation, focusing on investigations in response to allegations or complaints and thematic investigations. The second part of this section examines some of the methods used by overseers to scrutinise international intelligence cooperation, these include: hearings, documentary analysis, interviews, sampling, and direct access to databases.

INVESTIGATIONS IN REACTION TO ALLEGATIONS OR COMPLAINTS

Oversight bodies have most commonly examined international intelligence cooperation in reaction to allegations/revelations about wrongdoing that includes elements of cooperation with foreign services. In these circumstances, investigations may centre on a particular practice or case, such as the UK ISC's examination of the role of the UK services in rendition (see Box 7.2) and the Australian IGIS's investigation of actions of Australian officials relating to the arrest and detention overseas or Mr. Habib (see Box 7.6). Elsewhere, the Norwegian EOS Committee addressed aspects of cooperation in the Treholt case, which was ostensibly about the legality of police security service surveillance of one individual in the 1980s but involved close cooperation with a foreign service.[13] Overseers normally undertake reactive investigations on their own initiative, on the basis of a complaint, or when requested to do so by parliament or a responsible minister.

Box 7.2: UK Intelligence and Security Committee's investigation on rendition (2007)

Initiated by the Committee following allegations in the media, this inquiry assessed the UK intelligence services' knowledge of and/or involvement in the rendition of suspected terrorists by US intelligence services. Although the inquiry examined (and was precipitated by) allegations relating to UK involvement in specific cases of rendition, the Committee used this as an opportunity to examine the UK intelligence community's policies for sharing intelligence with foreign entities. This is a good example of how overseers can use investigations into specific cases to conduct broader assessments of a service's relations with foreign entities. In several cases, the Committee found fault with the services' failure to seek assurances regarding the treatment of persons about whom information was shared. However, it also concluded that US services had failed to respect caveats regarding the use of information shared by the British services. The report outlines recommendations for strengthening safeguards on intelligence sharing.[14]

Although aspects of this investigation and evidence given were subsequently criticised by another parliamentary committee and by the Court of Appeal,[15] the ISC's investigation was an important step leading to the reformulation and publication of ministerial guidelines on several aspects of international intelligence cooperation (see Box 6.7 in Chapter 6). There is an ongoing follow-up investigation examining the role of the UK government and security and intelligence services in relation to detainee treatment and rendition.

PERIODIC AND THEMATIC OVERSIGHT

Alongside their role in investigating particular cases or incidents, oversight bodies can also take a proactive approach to examining international intelligence cooperation. Indeed, it is good practice to scrutinise international intelligence cooperation in the absence of any specific allegations or reported problems. Accordingly, overseers may examine particular aspects of international intelligence cooperation (see above) on a periodic basis, usually annually. This is the practice of, for instance, Canada's SIRC, which now examines in-depth CSIS's activities at one foreign station each year, the Australian IGIS, and the Norwegian EOS Committee. Alternatively, oversight bodies may initiate, on an *ad hoc* basis, thematic investigations into services' cooperation with foreign entities or specific dimensions thereof. Box 7.3 provides examples of the international intelligence cooperation-related reviews that Canada's SIRC has conducted. The Dutch CTIVD has gone as far as to conduct a very broad ranging examination of the AIVD's cooperation with foreign entities. This included an assessment of laws, policies, and practice across many areas of international intelligence cooperation.[16]

Box 7.3: Examples of the Security Intelligence Review Committee's reviews of the Canadian Security Intelligence Service's cooperation with foreign entities (2004-2013)

- Review of a CSIS Foreign Station, 2013
- CSIS's Relationship with a Foreign Partner, 2011
- Review of CSIS's Relationship with a 'Five Eyes' Partner, 2010
- Review of CSIS's Role in Interviewing Afghan Detainees, 2010
- Review of CSIS Activities at a Foreign Station, 2008
- Review of CSIS's cooperation with and investigation of the intelligence services of a foreign country, 2007
- Review of CSIS's collaboration and exchanges of intelligence post-9/11, 2006
- Review of a Security Liaison Post, 2006
- Review of Foreign Arrangements with Countries Suspected of Human Rights Violations, 2005
- CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post, 2005
- Review of CSIS's Exchanges of Information with Close Allies, 2004
- CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post, 2004[17]

While overseers play a key role in reacting to allegations of malfeasance, proactive oversight of international intelligence cooperation offers a number of advantages. Notably, it enables overseers to scrutinise international intelligence cooperation outside of a context in which they are trying to determine what went wrong and who was responsible. Investigations in these contexts will often give rise to defensiveness on the part of the services and the executive, (sometimes unhelpful) media interest, and time pressure to provide a report. Thematic investigations can also be more comprehensive because they do not seek to respond to specific allegations – this can be useful in a field such as

international intelligence cooperation, where many oversight bodies are still developing their knowledge.

Finally, oversight bodies may also address international intelligence cooperation as one of many factors in a broader investigation that is not primarily about international intelligence cooperation. By way of example, Belgium's Committee I has touched upon international intelligence cooperation in several of its investigations, including on the services' work on non-conventional weapons, Jihadist extremism, and sects.[18]

Recommendations:

Oversight bodies should identify aspects of their services' cooperation with foreign entities to be monitored on a periodic basis.

Legislation should empower oversight bodies to undertake investigations on their own-initiative and overseers should use these powers to carry out thematic investigations into intelligence services' policies and practices relating to international intelligence cooperation.

Box 7.4: CTIVD investigation of the Dutch intelligence services' on the processing of telecommunications data including the exchange of data with foreign services[19]

Responding to the Snowden revelations on mass surveillance, the Dutch parliament asked the CTIVD to carry out a broad investigation of the services' (the General Intelligence Service and Defence Intelligence Service) collection, storage, and sharing of telecommunications data.

INTERNATIONAL INTELLIGENCE COOPERATION QUESTIONS

Among other issues, they examined the following aspects of international intelligence cooperation, both in law and in practice.

- Whether either service cooperated in the collection of telecommunications data in violation of Dutch law (including by allowing foreign services to tap telephone or Internet traffic in the Netherlands).
- Whether either service has used telecommunications data in violation of Dutch law when cooperating with foreign services.
- Whether either service sidestepped legal restrictions by requesting foreign services to collect data by a method they are not themselves permitted to use.
- The (legal) possibilities for and restrictions on the exchange of data with foreign services.
- The way in which the criteria for review laid down in the ECHR – necessity, proportionality, and subsidiarity play a role in the exchange of data with foreign services.

COMMITTEE METHODOLOGY

(1) Written questions

Sent written questions to the services in order to obtain a general picture of the subject matter. On the basis of the answers and exploratory talks with the services the Committee planned investigation days for each of the services.

(2) Investigation visits to the services

Interviews with the employees involved (mostly heads of the departments), discussing the data collection practices, and how data was stored and made accessible for internal use at the services.

Services provided a briefing on the use electronic applications/programmes for making data accessible and the possibilities they offer.

(3) Follow-up

Additional questions sent to the services – answered either in writing or at second interviews.

(4) Research in the intelligence services' electronic systems

Supplementary research in the systems of the services (using their powers of direct access to the services' systems).

METHODS

With the aim of assisting members and staffers of oversight bodies in scrutinising international intelligence cooperation, this subsection will highlight some of principal methods that have been used by overseers. These methods are not mutually exclusive and may overlap. This subsection includes two boxes illustrating how some of these methods can be brought together in the context of a periodic inspection (Box 7.5 on the EOS Committee) and in the context of an extensive inquiry (Box 7.6 on the Australian IGIS). Reference should also be made to Box 7.4 (above) on the Dutch CTIVD's recent inquiry into various facets of international intelligence cooperation.

Hearings

Holding formal hearings with service directors and relevant ministers is a method used by many oversight bodies and particularly parliamentary committees. Overseers sometimes use hearings to receive general updates on service activities, priorities, and threats. Insofar as it is consistent with their mandate, oversight bodies that stage such periodic hearings should seize this opportunity to request updates on international intelligence cooperation. Hearings may also be used to request information on specific issues or allegations as part of an investigation into a particular matter. In addition, oversight bodies hold less formal hearings to request informational briefings on, for example, aspects of international intelligence cooperation that overseers are seeking to understand.

Documentary analysis

Documentary analysis is a key part of any oversight work. Many investigations start with a request for relevant documentation and often a list of written questions. This would normally include any policies, internal guidance, or rules governing the areas of activity that are being examined. Notwithstanding any specific investigation, it is good practice for overseers to have ongoing access to these documents including any updates made by the services.

Interviews

Some oversight bodies interview personnel at different levels within intelligence services and associated executive bodies. Speaking to persons who have been directly involved in particular activities or operations may reveal more useful detail than hearings with service directors or ministers. Such interviews may help to reveal, among other things, how policies are interpreted and applied in practice, whether the legal framework is fully understood, and whether lower level personnel have any concerns about their work.

By way of example, in carrying out its reviews of the Dutch services' cooperation with foreign partners, the CTIVD interviewed service personnel in relevant departments across the AIVD, as well as speaking to relevant senior officials. Some oversight bodies can even interview persons under oath or affirmation in order to help ensure that they receive full and accurate information (see Box 7.6 for example). In addition to interviewing members of the services and related executive departments, overseers can also hold discussions

with outsiders. Such persons may include academic experts and members of civil society organisations, who may have information on particular activities or may simply provide an alternative perspective on, e.g. the legal standards that apply to international intelligence cooperation. Finally, where appropriate, overseers should interview persons (or their relations) who allege that they have been victims of intelligence service activities. In the context of international intelligence cooperation, this is especially important where any alleged mistreatment has occurred at the hands of a foreign intelligence service but there may have been some form of cooperation.

Sampling

Sampling involves the selection and examination of examples of documentation associated with a given intelligence activity. For instance, overseers may examine examples of personal data that has been sent to a particular foreign service, risk assessments on foreign services, or requests sent to a minister to authorise joint surveillance operations. Box 7.5 explains how Norway's EOS Committee uses sampling to scrutinise international intelligence cooperation as part of its periodic inspections.[20] Sampling does not mean that examples are selected randomly. Oversight bodies use knowledge from previous investigations to select examples of activities where there have been problems or where risks are seen to be high, e.g., information exchanges with foreign services that have poor human rights records. In most cases, oversight bodies have to scrutinise service activity on the basis of samples. They do not have the time or resources to examine all cases across all areas of intelligence service activity. The main exception to this is when overseers are examining a specific case or circumstances that require scrutiny of all relevant documents (see, for example, Box 7.6).

Box 7.5: EOS Committee's use of sampling during inspections

During its periodic inspections of the intelligence services, the EOS Committee habitually reviews information that is sent to foreign intelligence services. To keep this task manageable, the Committee requests a list of new and updated files and all personal data correspondence with foreign services (since their last visit). Members then select a sample based on particular foreign partners, individuals, or types of personal data. Using its direct access to the PST's electronic databases, the Committee examines relevant data to assess whether or not the service has complied with relevant regulations and policies.[21]

INSPECTION VISITS

Most oversight bodies have the power to conduct inspections of intelligence service premises. Briefings, interviews, and inspections of information systems often take place with the context of scheduled visits. Some oversight bodies, such as the EOS Committee in Norway, also have the power to make unannounced visits to the intelligence services if they consider it to be necessary. This is a tool that is unlikely to be used often, but it may be effective in situations in which overseers have concerns that the services have not be entirely forthright about a given programme or activity.

DIRECT ACCESS TO ELECTRONIC DATABASES

In some circumstances, direct access to the relevant intelligence services' electronic (and paper-based) information systems may enable oversight bodies to gain access to information relevant to their scrutiny of international intelligence cooperation (and other areas of services' work). This entails overseers accessing information themselves without requesting it from services, normally from their own offices within intelligence services. Several non-parliamentary expert oversight bodies (including Canada's SIRC, Norway's EOS Committee, and the Netherlands' CTIVD) use this tool. Whether or not direct access is a necessary tool for an oversight body may depend on the scope of its mandate, including whether it has a mandate to scrutinise operational matters.

The utility of direct access may, however, depend on how information is organised within an intelligence service. Information about international intelligence cooperation is sometimes fragmentary and scattered across different file management systems. For example, information pertaining to or derived from international intelligence cooperation may be included, *inter alia*, in files relating to immigration security assessments, security clearance processes, surveillance operations, and files on strategic issues. Accordingly, oversight bodies need well trained staff or technical advisers who know what to look for within such systems.

Granting overseers the power to view information directly – without having to request it from services – helps to give effect to overseers' statutory powers to access information. When overseeing international intelligence cooperation, direct database access reduces the potential problems caused by the third party rule (see below) because overseers do not need to ask services in order to view information shared by foreign partners. Such access is, nevertheless, a sensitive issue in the context of international intelligence cooperation because some services may contend that foreign partners will refuse to share information if overseers have direct access to information shared by them. For the reasons outlined in the next section, such concerns (real or exaggerated) cannot be determinative of the powers or methods available to overseers.

Oversight bodies must, however, recognise that direct access is an extremely powerful tool that must be used with caution and self-discipline. Overseers should not simply "go fishing" for information; information should only be accessed within the framework of an investigation or inspection. It is good practice for overseers to notify services (and generally ministers) when they commence investigations/reviews and ordinarily to inform them of decisions to access information. This is necessary not only for building trust between overseers and services but also because overseers often need services' assistance in navigating and interpreting electronic information systems. In view of the sensitive nature of direct access, it may be best introduced once an oversight body is well established and has developed a relationship of trust with services it oversees.

Box 7.6: Methodology used by Australian Inspector General for Intelligence and Security (IGIS) in the Habib Inquiry

This box details the comprehensive methodology adopted by the IGIS (an expert non-parliamentary oversight body) in its investigation into the actions of Australian officials relating to the arrest and detention overseas (including in Pakistan, Egypt, and at Guantanamo Bay) of an Australian citizen from 2001-2004. Cooperation with foreign services was an important component of the investigation.

Request for documentation

The IGIS started by briefings service directors on the inquiry and requesting specific categories of document including.

- Any *communications* between any representative, agent, official, or employee of any service of Australia, the USA, Pakistan, Egypt, and the UK between 1 July 2001 and 1 July 2005 concerning or relating to Mr Habib.
- All *policies, procedures and guidance material* (current and those in force at the relevant time) relating to various aspects of international intelligence cooperation including, *inter alia*, information sharing with foreign organisations about persons (likely to be) in detention and service involvement in questioning persons detained overseas.

Direct inspection of service files

An analysis of this documentation resulted in requests for additional information and direct inspection of service files/electronic systems by IGIS staff in order to search for additional pertinent information such as emails, notes and legal advice.

Interviews

The IGIS used her investigative powers to summon 24 currently or previously serving government (including intelligence service) officials for questioning under oath or affirmation. Relevant persons were interviewed in order to clarify information or supplement the documentary record, and/or where it was clear that a person had played a central role in events.[22]

7.4 Access to information by overseers

Overseers need access to information about the organisations and activities they are mandated to oversee. It is axiomatic that overseers cannot conduct scrutiny, draw conclusions, and hold people to account if they do not have access to all relevant information. An oversight body's information requirements are a function of its mandate, and it is for overseers to determine what information is necessary in order to for them to fulfil their mandates. Oversight based on incomplete access to information can result in misleading conclusions and may give rise to the misconception that services are being held to full account. The indispensable nature of full access to information relevant to an oversight body's mandate has been recognised in, *inter alia*, the *UN compilation of good practices on intelligence services and their oversight*, the CoE Commissioner for Human Rights' recommendations and the *Tshwane Principles on National Security and the Right to Information*. As has the need for access to information by overseers to be underpinned by statutory provisions and buttressed by appropriate investigative powers.[23]

In spite of the importance of access to information by oversight bodies seeking to scrutinise international intelligence cooperation, they can still face obstacles in this regard. Because an increasing proportion of the information held by many intelligence services is of foreign provenance (see Chapter 2), obstacles to overseers viewing information about or from international intelligence cooperation is likely to erode oversight and intelligence accountability, more generally.[24] Limitations on access also harm the scrutiny of other areas of services' work, which may be ostensibly domestic but are "contaminated" by foreign information. This section will highlight three significant restrictions on oversight bodies' access to information in this area: statutory restrictions, the third party rule, and technological challenges.

Before looking at the obstacles to access, it is important to note that cooperation with foreign services is among the most sensitive and secretive areas of intelligence services' work. It is, therefore, understandable that services closely guard information pertaining to or derived from these relationships. The potential harm that could be caused by the unauthorised or unintentional revealing of information from a foreign partner should not be dismissed lightly. Aside from the obvious privacy and personal safety implications certain types of information being revealed, breaches of foreign services' confidence can lead to a withdrawal of cooperation and the benefits that it brings. It is, therefore, essential that oversight bodies adopt appropriate security procedures and act with the utmost professionalism in handling information from or pertaining to relationships with foreign partners.

STATUTORY RESTRICTIONS

Although it is recognised as good practice for the law to grant oversight bodies unfettered access to information that they deem relevant for the fulfilment of their mandate, some states limit overseers' access to information on international intelligence cooperation. First, laws regulating oversight bodies sometimes explicitly prevent an oversight body from viewing information provided by a foreign entity. This is the case with regards to parliamentary oversight committees in Australia, France, and Serbia, for example.[25] Second, more commonly, laws include general restrictions on access to operational information by oversight bodies. In some systems, such as South Africa, information relating to cooperation with foreign entities is considered to be operational information. As a consequence, overseers may not access any information relating to international intelligence cooperation. Finally, some national laws contain provisions granting the executive broad discretion to determine what information can be provided to an oversight committee. Such discretion may be exercised in order to bar an oversight body from examining information relating to international intelligence cooperation.

Statutory limitations do not necessarily undermine oversight, as long as there is another external oversight body that has full access to such information (if necessary) and provided that any limitations do not preclude the oversight body from fulfilling its legal mandate. This is the case in both Australia and South Africa, where the parliamentary oversight committee's access to information is limited but a non-parliamentary expert body (an inspector general) has full access to all relevant information. It is of fundamental

importance that there is at least one external oversight body with access to the information necessary to scrutinise the aspects of international intelligence cooperation discussed in this chapter.

Recommendation:

Oversight bodies should identify aspects of their services' cooperation with foreign There should be at least one external oversight body that has full access to information held by the intelligence services, including information from or pertaining to international intelligence cooperation, which it considers to be relevant to the fulfilment of its mandate.

THIRD PARTY RULE

The *third party rule* or the *principle originator control* is the cornerstone of information sharing between services. It stipulates that information provided by a foreign entity cannot be transmitted to any third party or used for any other purpose that was not agreed upon the transfer of the information without the prior consent of the originator. It is intended to ensure that services retain a measure of control over information they send to foreign partners, including to prevent it from being transmitted to a third party that may use it in contravention of human rights. However, it can also serve to constrain an oversight body's access to information and, thus, its capacity to oversee a particular matter. This may happen if services and/or their partners view oversight bodies as third parties. Such an interpretation would imply that a service would need to seek the permission of a foreign partner before its own oversight could view information provided by that partner.

A process of seeking and granting such permission from foreign partners in order for oversight bodies to access information is likely to be unworkable, and it also has the potential to seriously undermine oversight. First, applying the third party rule to oversight bodies grants foreign services an effective veto on the scope of intelligence oversight in another state. A foreign partner may simply refuse to grant permission in order to prevent possible scrutiny of, for example, information sharing in a relation to a particular person. Secondly, a system that places intelligence services in a position in which they effectively have to seek permission in order to be fully scrutinised is seriously open to abuse. Services could (mis)use the third party rule to shield certain activities or files from external scrutiny. It is not difficult to imagine that – faced with a request from its overseer to view foreign information – a service could ask the question and provide the answer (no) when "seeking" the requisite permission from that foreign partner (i.e. they would suggest/invite the refusal of permission). Finally, few services would wish to suffer the reputational consequences of seeking permission for its overseers to examine a partner's information. Aware of these sensitivities, many overseers would refrain from requesting their services to submit requests to a foreign partner.

If applied in this way, the third party rule may seriously undermine external oversight of international intelligence cooperation. Addressing this concern, the Parliamentary Assembly of the Council of Europe has passed a resolution declaring that, "It is

unacceptable that activities affecting several countries should escape scrutiny because the services concerned in each country invoke the need to protect future co-operation with their foreign partners to justify the refusal to inform their respective oversight bodies."[26]

An increasing number of oversight bodies refuse to accept that they are third parties and/or that their services need to obtain the permission of foreign partners before their overseers can view information. Institutions such as the SIRC, CTIVD, and EOS Committee have taken the position that statutory provisions granting them access to all relevant information held by services override any limitations that may arise from the third party rule. Council of Europe institutions have endorsed this approach (see Box 7.7).

Box 7.7: Access to information by overseers and the third party rule: Council of Europe recommendations

In 2015, two Council of Europe institutions have made pronouncements on the need for access to information by oversight bodies to be unimpeded by the third party rule. The Parliamentary Assembly (made up of more than 600 parliamentarians from 47 states) passed a resolution stating:
"Those responsible for national control [oversight] mechanisms must have sufficient access to information and expertise and the power to review international co-operation without regard to the 'originator control' principle, on a mutual basis;"[27]

For his part the Commissioner of Human Rights of the Council of Europe has recommended that member states:
"Ensure that access to information by oversight bodies is not restricted by or subject to the third party rue or the principle of originator control. This is essential for ensuring that democratic oversight is not subject to an effective veto by foreign bodies that have shared information with security services. Access to information by oversight bodies should extend to all relevant information held by security services including information provided by foreign bodies."[28]

When drafting statutory provisions on oversight, legislators may need to be more explicit about the fact that the right of overseers to access information applies regardless of its provenance. If they have access to information shared by foreign entities, oversight bodies are subject to the third party rule, meaning that they can use the information as part of their functions but would not be permitted to disseminate such information without the requisite permission.

Recommendation:

The third party rule or control principle should not be permitted to override statutory provisions granting oversight bodies access to information necessary to fulfil their mandates. Parliamentarians should consider making it explicit in legislation that oversight bodies' access to information is not constrained by or subject to the third party rule.

Some intelligence services have legitimate concerns that overseers accessing information shared by foreign partners may lead these partners reducing information sharing. Both services and their overseers have responsibilities in allaying such concerns. For their part, services may be able to do more to present their overseers as reliable professionals who can be trusted with highly sensitive information and will respect the third party rule in the same way as insiders within their services. Intelligence services should consider inserting into memoranda of understanding or cooperation agreements with foreign services a clause highlighting the fact that cooperation may be subject to scrutiny by its oversight body.

Overseers can buttress their position by developing and maintaining reputations that support favourable assessments of their reliability and professionalism. Forging links with their contemporaries in foreign states may help in this regard (see below). Oversight bodies may be able to reassure their own services of the quality/reliability of oversight bodies in relevant partner countries. Services that are themselves subject to robust external scrutiny are likely to be more accepting if their partners are subject to similar oversight requirements that may entail shared information being viewed by overseers.

Recommendation:

Consideration should be given to requiring intelligence services to include in their agreements with foreign partners a clause stating that cooperation may be subject to scrutiny by a particular oversight body.

TECHNICAL DIFFICULTIES

Modern intelligence service activity, including some aspects of international intelligence cooperation, includes the use of extremely complex technology. This is particularly true of the systems used for collecting and sorting signals intelligence, as well as for storing information. Overseers are unlikely to be experts on such technology, and it may, therefore, be difficult to understand the scope, functions, and capabilities of such systems. This limitation makes it difficult to scrutinise activities that either use or are recorded through complex technology, which continues to evolve rapidly.

Legal powers to access information have limited practical value in overseeing, for example, joint signals intelligence collection or the exploitation of joint database systems if overseers cannot comprehend and interpret the capabilities of such systems. There is also the problem of volume; enormous quantities of information are collected (including through international intelligence cooperation) and shared with partners. It is challenging for overseers to know what to look at and what to look for.

With these technical challenges in mind, overseers will need to work closely with services to better understand their systems and technology. The availability of independent technological expertise can be invaluable, particularly when conducting inspections or database searches. The EOS Committee in Norway, for example, has a policy of hiring a

security-cleared technical specialist to advise on technical matters.[29] Such advisers can assist overseers in identifying relevant questions to ask or databases to examine, and they may also make proposals on how services' systems can be made more accessible to overseers. Hiring a technical adviser is likely to be especially useful for parliamentary oversight committees whose members have many other commitments and limited time to become acquainted with the complexities of intelligence work.

Recommendations:

Legislation should empower oversight bodies to hire security-cleared technological experts to assist them in understanding and assessing complex systems for the purposes of their oversight.

Additional resources should be allocated to oversight bodies to enable them to engage staff or external experts to assist them in understanding complex technology used by intelligence services, including in their cooperation with foreign partners.

7.5 Role of overseers in improving transparency of international intelligence cooperation

While much of the secrecy surrounding international intelligence cooperation is justified, governments, services, and overseers should consider what additional information about international intelligence cooperation might be placed in the public domain without negative consequences. Increased transparency is important because it helps to clarify, in general terms, what services do in their relations with foreign partners and, perhaps more importantly, what they are not permitted to do. This helps to provide the public with assurances about what is being done in its name, and it may serve to reduce conjecture about the activities of services.

Recommendations:

Consideration should be given to making general information about international intelligence cooperation public, including relevant ministerial directions or guidelines and oversight bodies' reports on international intelligence cooperation.

Overseers should encourage the executive and services to improve transparency in relations to international intelligence cooperation.

Oversight bodies have an important responsibility in this regard because they can take the lead in getting the executive and/or services to recognise the value of disclosing information. The UK ISC was instrumental in pressing the government to publish guidelines for intelligence officers and armed forces personnel on the detention and interviewing of detainees overseas, and on the exchanges of intelligence relating to detainees.[30] Similarly, Norway's EOS Committee succeeded recently in getting the Norwegian Intelligence Service to release in guidelines on their disclosure of personal data to foreign services (an extract from these guidelines is provided in Chapter 6, Box 6.4).[31]

Alongside promoting greater transparency on the part of services, overseers should also endeavour to publish details of their own work in scrutinising international intelligence cooperation. The release of such information is important for educating the public on how international intelligence cooperation is regulated, as well as for demonstrating to the public that services' relationships with foreign partners are being examined. In countries in which aspects of international intelligence cooperation have given rise to allegations of serious wrongdoing, this role of overseers becomes even more significant. When drafting reports on thematic or case/incident-specific investigations relating to international intelligence cooperation, overseers should strive to develop a public version, while still leaving scope for classified findings and recommendations. The Dutch CTIVD has taken a pioneering approach in this regard: it drafts public reports with classified annexes. The CTIVD's 2009 report on the AIVD's cooperation with foreign services remains the benchmark for oversight bodies providing detailed public reports on their scrutiny of international intelligence cooperation. This report has genuine utility for persons seeking to better comprehend international intelligence cooperation and how it can be regulated and overseen. By contrast, oversight reports that are only released following freedom of information requests (and heavily redacted) are of limited value for public education and assurance.

7.6 International cooperation between external oversight bodies

External oversight bodies (parliamentary and non-parliamentary) already engage in multilateral and bilateral exchanges. Examples include periodic meetings with national parliamentary oversight committees organised by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs; the annual Southeast European Parliamentary Oversight Bodies' Conference; the biennial International Intelligence Review Agency Conference (IIRAC); and the (now defunct) Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the European Union Member States. Such meetings occasionally address specific themes (including international intelligence cooperation) and common challenges faced by overseers. Further consideration should be given to using these meetings to address common challenges in specific areas of intelligence activity, such as international personal data sharing.

Informal meetings between similar oversight bodies, belonging to states that have close relationships and similar oversight models, allow more in-depth discussions and have addressed issues such as oversight methodologies and common challenges. These discussions do not involve the exchange of any classified information. In addition to gaining insights into different approaches to oversight, such exchanges may also help to develop the trust and credibility of oversight bodies among a group of states whose services cooperate closely. This may, in turn, reduce any concerns about overseers having access to information their services receive from foreign partners (see above).

There is no evidence of any oversight bodies cooperating on the oversight of particular instances of international intelligence cooperation, let alone exchanging sensitive

information. Given that intelligence services cooperate primarily to get better access to information to enable them to fulfil their mandates, it may seem logical for oversight bodies to follow suit. The rationale for overseers cooperating across borders would be broadly similar – to secure improved access to information in order to improve their oversight. When scrutinising international intelligence cooperation, overseers are often attempting to oversee their services' involvement in activities that involve authorities from one or more other states. They do not have access to foreign intelligence officials and cannot access information held by foreign services. This inevitably means that overseers are faced with an "incomplete factual landscape" that can undermine their ability to fully investigate and draw and conclusions about a given activity or incident.[32] The question arises as to whether oversight bodies could cooperate to overcome this challenge.

DIRECT INFORMATION EXCHANGES

It may be argued that, if intelligence services can transmit classified information to foreign counterparts, overseers should be permitted to do the same. There may be situations in which overseers could benefit from receiving information from foreign overseers as part of an investigation. Overseers in Country A might, for example, wish to ask foreign counterparts in Country B for information about what their services did with information sent by Country A's services. Alternatively, an oversight body in Country A may want information about what Country B's service did as part of a joint surveillance operation on the territory of Country A, in order to better understand what its own service's role.

While this logic may appeal, there are two serious shortcomings that render the sharing of classified information very unlikely. First, information (about and from intelligence services) accessed by oversight bodies does not become their information; the information is not theirs to share with foreign oversight bodies. It is hard to imagine an intelligence service acceding to a request from its overseer to transmit classified information to a foreign oversight body. Second, intelligence services would likely resist any sharing of classified information with foreign oversight bodies, not least because they have no relationship with these bodies and may not be able to trust them with information.

MUTUAL OVERSIGHT ASSISTANCE

A more realistic option is for oversight bodies to cooperate with their foreign counterparts through mutual requests to examine particular issues and the sharing of unclassified conclusions.[33] Two or more oversight bodies could devise a mechanism whereby they can request (or recommend) their counterpart(s) to examine a particular aspect of international intelligence cooperation from "their" side of a relationship. For instance, an oversight body in Country A (Oversight Body A) could ask its counterpart in Country B (Oversight Body B) to check whether outgoing information (from Service A) has been used in accordance with caveats, or whether incoming information (sent to Country A's service) was collected in compliance with the law. Alternatively, Service A might assert that it cannot allow its oversight body to see information because it was supplied by Service B, and Service B will not consent to this. Oversight Body A could then request Oversight Body B to: (a) check whether Service A submitted such a request, and (b) review a refusal

to grant such permission. Reports to the requesting oversight body need not contain any classified information – overseers can draft useful reports without classified information.

This type of cooperation could also be used to raise concerns with counterparts. Oversight Body A could flag issues with Oversight Body B regarding, for example, Service B's failure to submit written requests or sufficiently motivated requests for information to Service A, or its failure to attach reliability assessments to information sent to Service A. This could trigger additional scrutiny and, ultimately, rule/policy changes in Country B. This mechanism may not make a significant difference to oversight in the country whose oversight body makes the request or flags a concern. It could, however, help to promote better oversight on both sides of an intelligence cooperation relationship. In order for such cooperation to function, oversight bodies and their services would need to have close relations, such as those amongst the Five Eyes partners. It would also be contingent on their being oversight bodies of similar stature and comparable mandates on both sides of a relationship.

Recommendations:

Oversight bodies in states whose intelligence services cooperate with each other should work with their foreign counterparts to consider the possibility of developing processes for:

a. alerting each other to areas of mutual concern in the of the cooperation between their services, and
b. requesting that their foreign counterpart investigate and provide unclassified reports on specific issues of mutual concern that arise on the counterpart's side of an international intelligence cooperation relationship.

ADVICE AND SUPPORT AND TO OVERSIGHT BODIES IN EMERGING DEMOCRACIES

A number of European oversight bodies provide regular support to their counterparts in post-conflict and post-authoritarian states. Under the auspices of organisations such as DCAF and the OSCE, members and staff of long-established oversight bodies contribute to roundtable discussions and policy publications with the aim of sharing their expertise. Such assistance is especially important given that much of the support provided (by intelligence services) to intelligence services in these countries focuses on enhancing operational capacity.

It is important to recall that oversight bodies provide their support voluntarily, and this not part of their mandates. In order for this highly beneficial cooperation between more established oversight bodies and their newly created counterparts to continue, additional resources will need to be allocated to this work.

Recommendation:

Consideration should be given to providing oversight bodies with additional staff and resources to enable them to continue to provide advice and support to oversight bodies in emerging democracies. Such staff could also facilitate additional cooperation with well-established foreign counterparts.

Endnotes

1. See further: Aidan Wills, "European Parliament and Parliamentary Assembly of the Council of Europe Inquiries into Intelligence and Security Issues," in *Commissions of Inquiry and National Security*, eds., Mark Phythian and Stuart Farson, (Santa Barbara CA: ABC Clio, 2011).
2. See, for example: UK, Intelligence and Security Committee, *Rendition*, (London: HMSO, 2007), CM 7171; Canada, Security Intelligence Review Committee, *CSIS's Role in Interviewing Afghan Detainees*, 4 July 2011; Australia, Inspector General for Intelligence and Security, *Inquiry into the actions of Australian government agencies in relation to the arrest and detention overseas of Mr Mamdouh Habib from 2001 to 2005*, Public Report (Canberra: IGIS, 2011). [hereafter: Habib Inquiry].
3. Canada, *CSIS Act 1984*, s38(3).
4. See also the list put forward by the Commissioner for Human Rights of the Council of Europe: *Democratic and effective oversight of national security*, Issue paper, CommDH/IssuePaper (2015)2, (May 2015). Recommendation 5.
5. For further discussion, see: Aidan Wills, "Financial Oversight of Intelligence Services," Tool Eight in *Overseeing Intelligence Services: A Toolkit*, eds. Hans Born and Aidan Wills, (Geneva: DCAF, 2012).
6. Belgium, Standing Intelligence Agencies Review Committee (Committee I), *Rapport d'activités 2008*, (Brussels: Intersentia, 2009), 46, 52.
7. Kent Roach, "Overseeing Intelligence Sharing," Tool Seven in *Overseeing Intelligence Services: A Toolkit*, eds. Hans Born and Aidan Wills, (Geneva: DCAF, 2012).
8. The Netherlands, Review Committee on the Intelligence and Security Services, *Review report on the cooperation of GISS with foreign intelligence and/or security services*. See also, Norway, EOS Committee, *Annual Report 2005*.
9. Norway, EOS Committee, *The EOS Committees oversight of information exchange with cooperating foreign services*, Memo for DCAF, August 2013; EOS Committee, *Annual Report 2011*.
10. Australia, Inspector General for Intelligence and Security, *Annual Report 2010-2011*, (Canberra: IGIS, 2011), 25; Canada, Security Intelligence Review Committee, *CSIS Liaison With Foreign Agencies – Review of the SLO Post*, SIRC Study 2005-02.
11. Australia, Inspector General for Intelligence and Security, *Annual Report 2011-2012*, (Canberra: IGIS, 2012), 24; and *Annual Report 2010-2011*.
12. For a detailed overview of this issue, see: Aidan Wills, "Financial Oversight of Intelligence Services." (Geneva: DCAF, 2012).
13. EOS Committee, *The EOS Committee's investigation into the methods used by the Norwegian Police Surveillance Service (POT) in the Treholt case*, A Special Report to the Storting, (Oslo: 2011).
14. United Kingdom, Intelligence and Security Committee, *Rendition*.
15. United Kingdom, Joint Committee on Human Rights, *Twenty-Third Report - Allegations of UK Complicity in Torture*, (London: HMSO, 21 July 2009), paras 59-66; Mohamed, R (on the application of) v Secretary of State for Foreign & Commonwealth Affairs [2010] EWCA Civ 65, para. 168.
16. The Netherlands, Review Committee for the Intelligence and Security Services (CTIVD), *Review report on the cooperation of GISS with foreign intelligence and/or security services*.
17. Canada, Security Intelligence Review Committee website: http://www.sirc-csars.gc.ca/opbapb/lsrlse-eng.html.
18. Committee I, *Rapport d'activités 2008*, (Brussels: Intersentia, 2009), 46, 52; *Rapport d'activités 2010*, ((Brussels: Intersentia, 2011), 22-23; *Rapport d'enquête sur le suivi de l'islamisme radical par les services de renseignement*, (Brussels, 2007), para.9.5.
19. CTIVD *Review Report on the processing of telecommunications data by GISS and DISS*, CTIVD NO. 38, 5 February 2014, vi-xi, 1-9.
20. See also: CTIVD, *Review report on the cooperation of GISS with foreign intelligence and/or security services*, 1.
21. EOS Committee, *Annual Report 2003; Annual Report 2011*.
22. Australia, Inspector General for Intelligence and Security, *Habib Inquiry*. 14-19.
23. UN 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," 17 May 2010, A/HRC/14/46; Commissioner for Human Rights of the Council of Europe: *Democratic and effective oversight of national security*, Issue paper, CommDH/IssuePaper(2015)2, (May 2015). Recommendation 14; *Global Principles on National Security and the Right to Information (Tshwane Principles)*, adopted on 12 June 2013 in Tshwane, South Africa.

24. See for example: Alasdair Roberts, *Blacked Out: Government Secrecy in the Information Age*, (Cambridge: CUP, 2006), 263; Alasdair Roberts, "ORCON Creep: Information Sharing and the Threat to Government Accountability," *Government Information Quarterly* 21, no. 3, 2004.
25. France, *LOI n° 2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement*, Art 6.III; Serbia, *Law on the bases regulating security services of the Republic of Serbia, 2007*, Article 19; Australia, *Intelligence Services Act* 2001(as amended), Schedule Part 1a.1, and Part 1.1.
26. Parliamentary Assembly of the Council of Europe, *Resolution 1838* (2011), para 7.
27. Parliamentary Assembly of the Council of Europe, *Resolution 2045* (2015), para 19.2.
28. Commissioner for Human Rights of the Council of Europe, *Democratic and effective oversight of national security*, Recommendation 16.
29. Norway, EOS Committee, *Annual Report 2013*.
30. United Kingdom, Cabinet Office, *Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, on the Passing and Receipt of Intelligence Relating to Detainees*, (London, July 2010); Letter from the Chairman of the Intelligence and Security Committee to the Prime Minister, 23 April 2009; and UK, Intelligence and Security Committee, *Annual Report 2012*, (London: HMSO, 2013), para 136.
31. See, Norwegian Ministry of Defence, "Supplementary provisions concerning the Norwegian Intelligence Service's collection of information relating to Norwegian persons abroad and the disclosure of personal data to cooperating foreign services," adopted by the Ministry of Defence on 24 June 2013; See also, EOS Committee, *Annual Report 2011* and *Annual Report 2012*.
32. Andrea Wright, "Fit for Purpose? Accountability challenges and paradoxes of domestic inquiries," in *International Intelligence Cooperation and Accountability*, eds., Hans Born, Ian Leigh and Aidan Wills, (London: Routledge, 2011), 177-179.
33. Craig Forcese, "The collateral casualties of collaboration: the consequences for civil and human rights of transnational intelligence sharing," and Aidan Wills and Hans Born, "Formidable challenges and imperfect solutions," in International Intelligence Cooperation and Accountability in *International Intelligence Cooperation and Accountability*, 89-91.

8

Role of Courts in International Intelligence Cooperation

8.1 Introduction

The judiciary is an essential institution of the state, vital to upholding the rule of law, constitutionalism, and the protection of human rights. Apart from their technical ability in providing definitive interpretation and application of legislation and constitutional texts, courts provide an independent view of contested questions in a way that other state institutions cannot and act as the ultimate guarantee against the abuse of power for the protection of the individual.[1] In times of crisis and international conflict, this role is more important than ever.

Legislators and policy-makers need to be sensitive not only to the need to safeguard international intelligence cooperation, but also to the important role that courts play in protecting constitutional and human rights when action based on cooperation puts them at risk. A better understanding of the role of courts in this field is, therefore, an advantage. Moreover, courts themselves can benefit from examining practices that have been adopted in other jurisdictions to tackle common concerns in handling international intelligence cooperation.

This chapter first describes the different approaches that states take to intelligence material when it comes to legal proceedings. It will then deal with the various contexts

in which the courts may be engaged in adjudicating matters that touch on international intelligence cooperation at the domestic and international levels. It then examines some of the barriers to bringing legal proceedings concerning cooperation, before moving on to consider means by which courts can scrutinise intelligence cooperation. Finally, the ways in which international courts and tribunals are engaged and some of the practices they have adopted in this field are then discussed.

8.2 Intelligence and the courts

The legal problems caused by the secrecy surrounding intelligence cooperation are a subset of a wider question that many different legal systems have grappled with in recent decades: how to reconcile the protection of national security with fair trial rights. Since this question underlies all attempts to deal with material relating to intelligence cooperation in the courts, some preliminary explanation of the different ways in which states approach secret evidence in relation to trials and the implications of these different approaches is necessary. The most common approaches (summarised in Box 8.1 below) are variants on three models: *exclusion*, where secret material is simply forbidden in a trial; *provisional or conditional exclusion*, where a process exists by which an initial claim of exclusion can be overridden or reviewed; and *conditional inclusion*, where a procedure exists for receiving such evidence under particular safeguards or protections.[2]

EXCLUSION

Where intelligence material is excluded from a trial, the State cannot rely on intelligence to found a criminal conviction. Such a position often goes hand-in-hand with a (desirable) limitation on the mandate of the intelligence services, confining their role to information-gathering, analysis, and dissemination for the purpose of protecting national security. In its favour, exclusion can be said to protect individuals, and in some, states can be seen as an outworking of the separation of powers doctrine. The consequence, for example in relation to prosecution of terrorists, is that apprehension may be delayed until initial intelligence has been confirmed by legally admissible evidence. However, in some cases of extreme sensitivity or where it is simply impossible to gather legally admissible evidence, prosecution may become impossible in practice. Concerns of this kind have led some states – notably the UK – to the development of alternative, non-criminal, legal procedures, such as terrorism control orders (and their successors), which interfere substantially with individual liberty, but which can be challenged only within a secure legal environment deemed to be more protective of sensitive intelligence. Similarly, in cases of alleged wrongdoing by state intelligence officials, exclusion can lead in effect to immunity from prosecution. An example is the quashing of the convictions in Italian courts in 2014 of two senior intelligence officials implicated in the rendition of Abu Omar from Italy by the CIA, following the upholding of state secrets claims.[3]

In *civil* proceedings, total exclusion of secret material may have other negative effects in preventing individuals from obtaining redress for alleged wrongs by intelligence services/officials for essentially procedural reasons. Controversially, US courts have accepted

Box 8.1: Intelligence material and the courts: Comparing different approaches

Country	Type of Proceedings	Details	Features
Exclusion Model			
United States	Civil	State secrets doctrine	A conclusive claim by the executive.
United Kingdom	Civil	Public Interest Immunity	Can be raised on ministerial authority but the court can decide to inspect the relevant material and can over-rule the claim, wholly or partially.
Provisional or Conditional Exclusion Model			
France	Civil and Criminal	Reference to the Commission consultative du secret de la défense nationale.	Classified material is excluded, but a court may request declassification of intelligence material by the Commission.
Germany	Civil	*In camera* review by Higher Administrative Court	Higher Administrative Court reviews contested material *in camera* and may have jurisdiction to quash a claim for non-disclosure.
Italy	Criminal	State secrets	The court or prosecutor may refer question on applicability to the information concerned to the President of the Council of Ministers (and then to the Constitutional Court).
Conditional Inclusion Model			
Netherlands	Criminal	Shielded Witnesses Act 2006	*In camera* and *ex parte* handling of intelligence evidence before a special examining magistrate.
Spain	Criminal	Expert intelligence evidence	Judicial doctrine allows reception of intelligence in terrorism trials from the police in the form of expert evidence.
United Kingdom	Civil	Closed material procedures under Justice and Security Act 2013	The court may apply the procedures, if satisfied, that sensitive information would be required to be disclosed and that it is in the interests of the fair and effective administration of justice. Proceedings are held *ex parte* with a special advocate representing the excluded party's interests. The court releases a summary of closed proceedings. Exceptionally, even the fact that CMPs have been used may be withheld.

that a claim of state secrets privilege is conclusive,[4] and the effect can be seen clearly in a succession of decisions in which US courts applied the state secrets doctrine to civil actions brought by individuals to sue officials and companies allegedly involved in their rendition by US agencies.[5] The danger in treating claims to evidential privilege as conclusive in this way is that it risks substantial injustice, in that a party with a sound legal claim against the government will be prevented from pursuing it because of suppression of available evidence. A variant on exclusion, particularly relevant to civil cases, is where a state claim of secrecy is conclusory, but the executive has a monopoly on initiating the claim and discretion over whether to do so. In such instances, there is a heightened risk of injustice and lack of accountability because the discretion can be abused to prevent embarrassment or exposure of wrongdoing.

PROVISIONAL AND CONDITIONAL EXCLUSION

Examples of *provisional or conditional exclusion* of secret material include those where the judge or a designated court may inspect the contested material and is able to overrule the secrets claim made by the executive. This is the case with claims of public interest immunity in civil cases in the UK (the doctrine cannot be used in criminal cases), which allow for judicial inspection of the contested material and weighing of the claim against other interests.[6]

Further examples of provisional or conditional exclusion can be found in German and Dutch law. In Germany, a refusal by the intelligence service or the Ministry of Interior to submit secret material that could be disclosed in court can be challenged under a procedure that allows the Higher Administrative Court to review the material in camera (it is not disclosed to the claimant, unless the exclusion is quashed).[7] In the Netherlands, the Administrative Division of the Council of State has declined to apply a legislative provision that gave exclusive competence to the intelligence service to determine if there were appropriate reasons to disclose documents in a civil case (the action was a challenge to refusal of security clearance for employment at an airport). It found that the right of fair trial required that the court, rather than the intelligence service, must be able to determine the necessity for non-disclosure.[8] As this decision shows, the strength of provisional or conditional exclusion is that in providing for independent assessment of executive claims it gives greater weight to the right of fair trial than it does to total exclusion.

Where a court finds that exclusion is justified under such a procedure, there is the reassurance that the secrecy claim has been confirmed by an independent body. If, on the other hand, the challenge is upheld, it may lead to the government seeking to settle or discontinue proceedings to avoid complying with an adverse judicial ruling to disclose intelligence to other parties. This option is not a possibility, however, when the government is only a third party to litigation, because as an intelligence partner it may have relevant information relating to proceedings that are brought against foreign officials or intelligence services.[9] This has been a partial explanation for the UK government seeking to regain a measure of control by introducing Closed Material Procedures under the Justice and Security Act 2013, described below.

Procedures that allow for the courts to seek a review from the executive of the decision to exclude secret material are comparable. For example, under the Italian Code of Criminal Procedure, a public servant must not disclose secret material in court by answering questions covered by state secrets. The relevant provisions require the prosecutor or judge to refer to the President of the Council of Ministers whether the material is so covered.[10] A negative response results in the material being treated as normal evidence. If the claim of state secrets is confirmed, however, the court may nonetheless refer the question to the Constitutional Court, which then assesses the validity of the claim. A somewhat similar process exists in France, where classified material is inadmissible in legal proceedings but under law No. 98-567 of 8 July 1998, a court may refer a request to declassify secret material to the *Commission consultative du secret de la défense nationale*.

CONDITIONAL INCLUSION

Examples of *conditional inclusion* of secret evidence are procedures that allow for the reception of intelligence material under protective conditions. The Netherlands has perhaps gone furthest in this regard, with the Act on Shielded Witnesses Law introduced in 2006 in *criminal* cases.[11] National Security is protected by the procedure under which the special examining magistrate (*rechter-commisaris*) may withhold information from disclosure to the public or the defendants.[12] Intelligence officers may be permitted to give evidence anonymously as shielded witnesses, *in camera* and *ex parte*, in a specialised court in Rotterdam. A list of questions is submitted to the special examining magistrate by the defendants and the trial judge, though neither attend, and with a subsequent transcript of the answers made available to the parties only with the consent of shielded witnesses. There is no appeal against the decision to grant anonymity. Inherent in the process are substantial restrictions on the defendant's rights to challenge evidence and on the trial judge's ability to assess the credibility of the shielded witnesses. The effect on the right to fair trial is therefore controversial.[13] Also controversial is the practice in the Spanish courts of receiving intelligence in terrorist trials from the police in the form of "expert evidence."[14] Since the material is not submitted directly by the intelligence service, but only indirectly through the police, the defendant's ability to challenge factual detail is constrained.

Recent legislation in the UK, specifically the Justice and Security Act 2013, introduces Closed Material Procedures (CMPs) in civil cases. These do not apply to criminal cases. The justifications for introducing CMPs were that disclosure of intelligence material in open court would endanger national security and intelligence cooperation. However, to wholly exclude it from consideration would prevent judges from taking important material into account or prevent the government from fully defending itself against allegations. Consequently, the legislation is intended to allow intelligence material to be considered under conditions of secrecy, which may include consideration of the material in the absence of the other party and their lawyers. However, special advocates, in the form of security-cleared lawyers, are permitted to participate and to challenge the relevance and admissibility of the intelligence material.[15]

In all three states, these procedures are controversial, and critics have argued the processes are inadequate to provide a fair trial to the other party from whom material is withheld.[16] In criminal trials, especially in the Dutch and Spanish examples, restrictions inherent in these procedures risk producing an inequality of arms between the prosecution and defence by effectively limiting the ability to cross-examine evidence that may be relied on by the court in reaching a conviction.

In terms of strengthening the accountability of intelligence services and ensuring that alleged wrongdoing can be investigated and remedied in an independent way, it is clear that legal procedures which provide for the provisional or conditional exclusion or the conditional inclusion of intelligence are preferable to its total exclusion. This places an onus on legislators and courts to devise processes by which intelligence can be handled securely in litigation while also protecting the right to fair trial as much as possible. A review of *Abuse of State Secrecy and National Security*, which was conducted for the Parliamentary Assembly of the Council of Europe Committee on Legal Affairs and Human Rights, underlies this approach. These basic principles are summarised below in Box 8.2.

Box 8.2: Parliamentary Assembly of the Council of Europe: Basic principles for judicial and parliamentary scrutiny of the secret services

1. There must not be any "areas removed from any kind of control," …. It must therefore be possible for the criminal and civil courts… to investigate serious allegations of crimes and human rights violations without being prevented from doing so… [reliance] by the very intelligence services being investigated, on state secrecy or national security to block access to relevant information.
2. The three powers of the state – the executive, the judiciary and parliament – are… jointly and equally responsible for safeguarding the state's interests and security. All three powers can and must make the necessary arrangements for secrets threatening state security not to be disclosed.
3. Breaches of the law and comparable abuses by state agents are not by their nature legitimate secrets. Even if there is no specific legislative provision on the subject, the courts have the right…. not to consider such facts as secrets worthy of protection by way of interpretation of the law..
4. To prevent legitimate secrets from being revealed because they are inextricably linked to illegitimate ones, courts… must foresee suitable procedures making it possible both to protect legitimate secrets and to prosecute the perpetrators of crimes and award damages to victims.
5. These principles also apply, and are particularly relevant, in the field of international co-operation in the fight against terrorism and organised crime. It is unacceptable for acts of co-operation, and in some cases complicity, between secret services in different states to escape the usual oversight to which they are subject in their own state. Increased co-operation between secret services … must go hand in hand with equivalent co-operation and mutual trust between oversight bodies.[17]

Note: additional references in the original to parliamentary scrutiny have been omitted from this summary.

Recommendations:

Legislators and courts should devise processes by which intelligence can be handled securely in litigation while also protecting the right to fair trial as much as possible. Such legislation or procedures should guarantee that restrictions only apply where strictly necessary, and that the final decision on disclosure is made by a court.

Any procedure adopted to protect classified information or intelligence cooperation relationships in litigation should not prevent access by a victim of human rights to an effective remedy or allow for suppression of information concerning gross human rights violations.

8.3 Domestic courts and international intelligence cooperation[18]

International intelligence cooperation can arise in legal proceedings in domestic courts in three basic ways. Firstly, there can be direct challenges to the legality of cooperation *per se*, ranging from constitutional, administrative or civil law challenges to the actions of the intelligence services, to criminal proceedings or civil actions against individual officials. Secondly, there can be indirect or collateral challenges, where the focus is the legality of action based on information derived from intelligence partners, for example, in the context of a terrorist prosecution or an immigration decision. Thirdly, there are cases where the focus of the litigation is the protection of information concerning intelligence cooperation per se, such as official secrets prosecutions or appeals against the withholding of information under freedom of information or data protection exceptions. These are not watertight categories, however. Access to information about intelligence cooperation may be a precursor to a direct or indirect challenge, for example.

CHALLENGES TO THE LEGALITY OF INTERNATIONAL INTELLIGENCE COOPERATION

Direct challenges to the legality of intelligence cooperation in the first category are most likely to take the form of constitutional or administrative law challenges to the actions of the intelligence services. Some examples are the challenges brought in the Canadian courts to the involvement of the services in interrogating terrorist suspects held abroad,[19] or to disclosure of intercept material to foreign intelligence services.[20] Somewhat similar challenges have been brought in the UK to the legality of the ministerial guidance issued to cover the conduct of intelligence officers dealing with intelligence partners, who have suspects in detention,[21] as well as to the alleged supply of locational information by GCHQ to the US for overseas drone attacks.[22] The question of the liability of the German government for permitting a US airbase on its soil to relay signals to coordinate drone attacks in Yemen has likewise arisen in the German courts.[23]

Civil litigation against the services or individual officials is another form of direct challenge.[24] Alternatively, in some states, there are specialist courts or tribunals in which complaints may be brought against the security and intelligence services. These may be the fora in which such direct challenges take place – the UK Investigatory Powers Tribunal

being one example. In rare instances, there may be criminal proceedings against individual officers, for direct or secondary involvement in kidnapping or torture for example.[25] In many cases, the "action" of the intelligence service challenged will be the decision to supply information or assistance to a partner intelligence service. The most serious examples would be where the intelligence supplied is claimed to have led to targeted killing,[26] extraordinary rendition, or the continued detention and questioning, involving torture or abuse of a person in the partner state. Other examples might include supply of information resulting in another state in prosecution, executive decisions concerning immigration or asylum, or financial penalties under anti-terrorism legislation such as sanctions that freeze assets.

Box 8.3: Italy: Abu Omar case[27]

On 17 February 2003, Osama Mostafà Hassan Nasr (known as Abu Omar), an Egyptian cleric who had been granted political asylum in Italy, was kidnapped in Milan by CIA agents and flown to the NATO Air Base in Ramstein, Germany. From there he was transferred to Egypt, where he was allegedly tortured. The kidnapping and transfer were part of the United States' 'extraordinary renditions' programme.

On 4 November 2009, the Tribunal of Milan convicted 22 CIA agents (two of whom also performed consular functions in Milan at the time of the kidnapping), one US military official, and two Italian secret services operatives[28] for their participation in this operation.[29] On 15 December 2010, the Court of Appeals of Milan confirmed the first instance judgment.

In appeals brought by the defendants, the Court of Cassation found that Italian criminal tribunals had jurisdiction over US military officials who were involved in an extraordinary rendition operation carried out in Italian territory which involved the crime of kidnapping, notwithstanding the Status of Forces Agreement.[30] It was irrelevant whether the actions occurred in the course of the officials' duties or whether the Italian Ministry of Justice conceded US jurisdiction.[31] The two defendants who were US consular agents did not enjoy immunity in the Italian courts under the Vienna Convention on Consular Relations,[32] since such immunity only applied to actions in the course of normal consular activities, and any authorisation by the Italian government did not confer immunity. Nor in their case was it established that under customary international law, state officials who had participated in an extraordinary rendition operation enjoyed functional immunity from the criminal jurisdiction of a foreign state.

Note: This box deals only with the proceedings brought against US officials in this instance. After a protracted series of legal challenges, state secrets doctrine was successfully invoked by Italian intelligence officials implicated in the affair to bar prosecution.[33]

INDIRECT CHALLENGES TO INTERNATIONAL INTELLIGENCE COOPERATION

Indirect challenges to decisions based on information derived from intelligence partners can be brought in a variety of ways.

They may take the form of constitutional and administrative law challenges to decisions based on intelligence received from foreign partner intelligence services, especially in immigration or anti-terrorism cases. Some states have specialist security-sensitive tribunals, such as the UK's Special Immigration Appeals Commission,[34] in which cases of this kind are heard. In jurisdictions in which judges are involved in the authorisation of the use of special powers of the security and intelligence services, questions about the legality of information received through cooperation may occur in the course of those closed proceedings, raised by the judge, or an independent or special advocate.

Indirect challenges may also arise in the course of criminal proceedings, especially terrorism prosecutions,[35] although it is uncommon for such prosecutions to be based solely or mainly on intelligence supplied by partners. The sensitivity of the foreign intelligence service that has supplied intelligence in such cases may effectively prevent a prosecution at all or lead to it being dropped.[36]

Other indirect challenges are to the impact of international intelligence cooperation considerations on unrelated decisions- such as the unsuccessful attempt by campaigners in the UK to challenge the dropping of a bribery investigation due to a threat from Saudi Arabia to withdraw intelligence cooperation if it continued.[37] International intelligence cooperation may also be an issue where a litigant is seeking the diplomatic protection of his or her government to intervene on their behalf with an intelligence partner.[38] One particular situation that has received detailed recent analysis concerns information supplied by foreign intelligence services that may have been obtained through the torture or ill treatment of a third person.[39]

SECRECY ABOUT INTERNATIONAL INTELLIGENCE COOPERATION

Cases in the third category, where the focus of the litigation is protection of information concerning intelligence cooperation per se, can arise across practically any of the situations described above. Criminal prosecutions for espionage, where it also affects an intelligence partner,[40] and for unlawful disclosure of information supplied by foreign governments may have this objective. Administrative appeals against freedom of information or data protection exceptions to protect foreign government information or information damaging to international relations are also within the third category.[41] Protections from disclosure in litigation for information that would be damaging to national security or foreign relations are commonplace in legal systems, for example through state secrets privilege.

8.4 Judicial inquiries

In addition to these court-centred treatments of international cooperation, mention should also be made of the fact that, in many states, senior judges are from time to time called upon by governments to conduct independent inquiries into matters of public concern related to security and intelligence.[42]

This is likely to occur where the investigation of some allegations involving human rights abuses is too complex for investigation by a parliamentary committee or where public confidence may require independent judicial investigations. A judicial inquiry can have several advantages. In many states, the stature and perceived impartiality of the senior judiciary instils public confidence in the investigation. Complex inquiries can benefit from the procedural and evidence-handling training of judges. Judges may be able to handle the questioning of senior politicians and officials with a detached authority that other institutions cannot attain.

These judicial inquiries may touch on questions dealing with cooperation, although when they do so the formal powers of inquiry will not be effective in compelling foreign governments or their intelligence services to give evidence (although they could agree to cooperate voluntarily). An example of an inquiry of this kind was the independent judicial inquiry in Canada conducted by Justice O'Connor to examine allegations of complicity by CSIS in rendition and torture in the case of Maher Arar.[43] Notwithstanding the failure of the US and Syrian authorities to cooperate, the Arar Commission produced a series of specific proposals to clarify the prevalent practice among intelligence professionals of the use of caveats, i.e. conditions restricting the use of information shared with a partner intelligence service.[44]

8.5 Difficulties of challenging international intelligence cooperation in the courts

There are undoubted obstacles to an individual even commencing legal proceedings to protect their rights, where there has been an infringement due to international intelligence cooperation. In many cases, the person may simply be unaware that action has been taken that concerns them. An exchange of personal data between intelligence partners or authorisation of surveillance, for example, may never come to his or her attention. Even if they do become aware, there may be a lack of knowledge regarding who is responsible for the interference with their rights or insufficient information to mount an effective legal challenge. If those hurdles are overcome, the gathering of evidence to discharge the burden of proof before a court is a real difficulty. For example, agents of foreign intelligence services are unlikely to answer to court orders.

Where proceedings have been instigated, however, there are further obstacles to redress in the courts for activities affecting individuals that involve intelligence cooperation.

Box 8.4: The O'Connor Commission of Inquiry into the disappearance of Maher Arar (Canada)[45]

Mr. Arar, a Canadian citizen of Syrian birth, was detained by US authorities while changing planes at John F Kennedy International Airport en route from Switzerland to Canada in September 2002. After being held in the US for 12 days, he was deported against his will to Syria where he was interrogated, tortured and held in degrading and inhumane conditions before being released in October 2003.

The O'Connor Commission concluded that Canadian officials in Project A-O, an investigative unit of the RCMP conducting an investigation into a suspected Al-Qaeda cell, had supplied inaccurate information to US agencies identifying Maher Arar as a terrorist suspect, whereas in fact he was a "person of interest" because of his acquaintance with a suspect.

While it stressed the importance of intelligence sharing both by domestic police and security agencies and internationally, the O'Connor Commission nevertheless proposed that in Canada's case it should be governed by clearer principles in the future. It recommended that these principles also be adopted by the Canadian Security Intelligence Service. The report provides important detail concerning the apparently widespread international practice of attaching "caveats" to intelligence, and it made important recommendations concerning the use of caveats in the future by Canadian services.[46] (The specific recommendations are discussed in Chapter 6).

Following publication of the O'Connor report in 2006 the Canadian Government agreed to pay $9.8 million in compensation to Arar.

PUBLIC INTEREST AND JUDICIAL DEFERENCE

Many states retain the ability to control or abort legal proceedings on grounds of public interest, whether directly, as in refusal to sanction prosecution or extradition of intelligence officials, or through control of evidence, which disallow certain forms of evidence relating to intelligence in the public interest under doctrines such state secrets privilege and public interest immunity.[47] Judges tend to be deferential to the executive in questions of national security where intelligence and foreign affairs mix.[48] The doctrine of foreign sovereign immunity may protect the intelligence services of foreign states from liability in a partner state.[49] In addition, the courts of some legal systems recognize that they should avoid questioning the acts of foreign states as a matter of international comity under the "act of state" doctrine. There are, however, limits to which this shields intelligence cooperation from scrutiny. Under English law, for example, in recent litigation concerning the alleged involvement of MI6 with US authorities in an alleged rendition the Court of Appeal has found that potential embarrassment to the UK government in its international relations is not a sufficient reason to decline jurisdiction, and that in any event the doctrine does not apply to the alleged acts of a foreign state outside its territory.[50]

Although there are good reasons for judicial deference where international intelligence cooperation is challenged directly or indirectly, this approach also carries dangers. Since, as noted in Section 8.6, courts in several states no longer automatically defer to other national security claims as they once did, there is the possibility that the executive might be tempted to invoke the risk of harm to international intelligence cooperation instead. There is also a risk of unnecessary claims. The partner intelligence service may not in the particular circumstances have an objection to the material being disclosed in proceedings. For this reason, it is good practice for intelligence services to check with their partners that caveats inhibiting disclosure in proceedings cannot be relaxed before asserting in proceedings that international intelligence cooperation will be harmed. In other cases, if more information was made available, it may be apparent that there would be clear case against disclosure in any event. Too ready acceptance of the case against disclosure by the courts may also incidentally weaken the position of overseers in requiring access of information about international intelligence cooperation.

EVIDENTIAL PRIVILEGE

Protections from disclosure in litigation for information that would be damaging to national security or foreign relations are commonplace in legal systems.[51] As noted in section 8.1, these doctrines predominantly apply to civil proceedings, although there may be similar limitations on disclosure in a criminal trial, making due allowance for the defendant's fair trial or due process rights. There are variations between jurisdictions over who can raise a relevant claim of privilege (the government only, as in the US or other parties, as in the UK) and over whether a claim is conclusive. The danger in treating claims to evidential privilege as conclusive in this way is that there is risk of substantial injustice in that a party with a sound legal claim against the government will be prevented from pursuing it because of suppression of available evidence. Judicial inspection and weighing of the interests for and against disclosure is a significant safeguard against the risk of excessive or self-interested claims on the part of the executive. Jurisprudence under Article 6 of the European Convention on Human Rights, which deals with the right to a fair trial, also leans against such conclusive claims to privilege and stresses the importance of judicial control of disclosure of information.[52]

INFORMATION LAW EXCEPTIONS

Chapter 5 discussed the widespread practice of including exceptions relating to intelligence cooperation in freedom of information and data protection legislation. The use of these exceptions is sometimes further protected by provisions requiring the court or tribunal to accept the word of a minister that harm of this type will be caused ("conclusive ministerial certificates"). Australia, Canada and New Zealand, also parties to the UKUSA alliance[53] (see Box 2.1 in Chapter 2), all have legislative provisions allowing for conclusive ministerial certificates relating to information the disclosure of which would allegedly damage international relations.[54] *Inter alia*, these provisions give assurance to the intelligence partners by effectively excluding the possibility that a court could ever order disclosure when a claim had been made that intelligence cooperation would be harmed.

It is likely that US concerns over Canadian legislation were a prime motivating factor behind the introduction of a procedure in 2001 whereby the Federal Attorney-General can issue a conclusive certificate for the purpose of protecting national defence or security or information obtained in confidence from another government.[55] A certificate of this kind discontinues proceedings before the Information Commissioner or the Federal Court, subject only to the Court's ability to check that the information falls within one of the prescribed categories. In practice, however, the procedure has not to date been used. The Australian conclusive certificate provisions are the most developed in providing for a modified form of review where a conclusive certificate is tabled.[56] This takes place before a specially constituted panel of the Administrative Appeals Tribunal, comprising of presidential members only and according to a reasonableness standard (whereas the normal standard is merits review).[57] Moreover, the minister may decide not to follow a decision to quash a certificate, in which case the Act provides for notice to parliament, in effect returning the issue to the political process.

There are clear dangers where the courts are obliged to accept ministerial certificates as conclusively preventing either a legal claim, such as for disclosure of information under freedom of information legislation, or under evidential privilege. This skews the balance of power between the executive and the judiciary and in effect puts the executive in the sole position of judging and being able in effect to prevent a party's legal claim against them.

8.6 Judicial examination of intelligence cooperation

Adjudication in litigation involving international intelligence cooperation is certainly challenging because of the mix of national security, defence and foreign policy that these cases present. National security and foreign affairs are fields in which courts in many jurisdictions have often in the past deferred to governments, especially in wartime. Nevertheless, and particularly since 9/11, judges in a number of states and in international tribunals have recognised that the issues are too important to allow a legal "black hole" to develop. This section, first of all, examines the general approach that courts can take to aid accountability in relation to international intelligence cooperation, before considering several specific practices that can be adopted that also assist this objective: a requirement to preserve intelligence, third party disclosure, "gisting," the use of an agreed hypothetical case, and, finally, assessment by the court of the effect of disclosure.

Especially relevant in this context is a 2009 decision of the German Federal Constitutional Court emphasising that the government could not decide unilaterally to withhold information from a parliamentary commission of inquiry examining alleged cooperation of the German services in the US programme of secret detentions and unlawful transfers of detainees. The inquiry, which sat between 2006 and June 2009, was hampered by numerous claims of state secrets made by the German government to limit the testimony of officials and to prevent access to documents. A group of Parliamentarians brought a largely successful challenge to the Federal Constitutional Court, which found that the executive claims to secrecy had been excessive and that the parliamentary commission

had a corresponding constitutional right to be informed of these matters. Although the Constitutional Court's decision came after the commission of inquiry mandate had expired, it nonetheless established some important principles relevant to future state secrets claims, described in Box 8.5.

Box 8.5: Parliamentary access to state secrets: The German Federal Constitutional Court's approach

- The government's interest in protecting its internal decision-making process must be weighed against the parliament's interest in being informed, with due regard to the separation of powers. This interest was especially weighty when it was a matter of detecting possible breaches of the law and like abuses within the government.
- Executive claims of state secrecy must be supported by specific and detailed reasons for withholding information so that the claims can be verified – ultimately by the Constitutional Court itself.
- The safeguarding of the state's interests, including its security, was equally and jointly assigned to the government and to the parliament by the constitution. The parliament and its organs were not to be regarded as third parties from whom information must be kept secret to protect the interests of the state.
- Information on contacts with foreign secret services was not automatically shielded from parliament's requests for disclosure. The reasons why publication of this information could be harmful to future co-operation between these services should have been explained.
- The mere fact that the publication of such information might embarrass the government did not constitute a danger to the interests of the state, but a consequence, ordained by the constitution, of the exercise of the right of parliamentary inquiry.
- There should be no "areas exempt from oversight" when it comes to investigating breaches of the law or like abuses… The government must not be in a position to determine the scope of an investigative mandate and of the inquiry commission's right to demand evidence, otherwise it would take control over its own overseers.
- While the preparation of government decisions and the decision-making process were generally part of the "central area of the executive's responsibility," that was not necessarily so once the decision has been taken and the case under consideration has played out. In an *ex post* assessment, however, the effect of allowing access to full information on similar future decisions must be considered.[58]

PRESERVING THE RECORD

Turning to specific practices that aid accountability through litigation, a requirement that domestic intelligence services must first of all preserve intelligence that has influenced decisions affecting an individual can partially offset the difficulties that litigants face in obtaining information. The Supreme Court of Canada found that CSIS owed a duty of this kind in the second *Charkaoui* case.[59] The Supreme Court found that, in order to have a fair trial of whether an immigration Security Certificate violated the petitioner's constitutional

rights, disclosure was necessary of the information on which the certificate had been based. The Court interpreted a duty in the CSIS Act 1984 to preserve intelligence to be inconsistent with CSIS's policy of destroying interview notes and only retaining a summary.

THIRD PARTY DISCLOSURE

Another strategy used by lawyers representing litigants, who claim to have suffered human rights abuses at the hands of foreign intelligence services, is to bring proceedings against domestic authorities for disclosure of any related intelligence they may have received from the services in the counties accused of wrongdoing that could assist the claim in foreign courts. This approach was used in the UK in the *Binyam Mohammed* case (see Box 8.6 below) and several other prominent cases.[60] From the point of view of protecting sensitive intelligence, such litigation can be seen as creating an invidious choice between disclosure in open court, use of various forms of closed proceedings designed to protect the intelligence, or negotiating settlement of the proceedings to avoid disclosure. In the UK, amending legislation has been introduced (the Justice and Security Act 2013, discussed in Box 8.1) that will have the effect that foreign intelligence material may no longer be disclosed in this way.[61] On the other hand, it can also be argued that a civil claimant should not in effect have to bear the cost of protecting intelligence in the form of restrictions of his or her rights.

"GISTING"

A possible alternative to disclosure of intelligence received from foreign intelligence services is for the services concerned to agree to summarise the material for the benefit of the court, if this can be done in a way that does not interfere with security. This is what happened in the New Zealand courts in the Zaoui case, wherein the protracted litigation surrounding the attempts of Ahmed Zaoui to resist deportation from New Zealand between his arrival in December 2002 and the lifting of security objections to his entry in September 2007.[62] According to material disclosed by the New Zealand Security Intelligence Service (NZSIS) during proceedings in 2004, NZSIS had instigated inquiries with 'liaison partners' in Belgium, France and Switzerland about Zaoui's activities since leaving Algeria in 1993.[63] These inquiries showed that he had twice been denied refugee status in Belgium, and that he had been "convicted in Belgium in 1996 of being a leader and instigator of a criminal association with the intention of attacking persons and property." They also showed that he had illegally entered Switzerland in 1997, an, he had been denied access by the Swiss government to fax, email, and use the internet, due to engaging in activities which were seen to endangering Switzerland's domestic and external security. He was then expelled from Switzerland.[64] The Belgian and Swiss partner services agreed to unclassified summaries of classified material being released to Zaoui's lawyers for the purpose of the New Zealand proceedings, and the NZSIS provided unclassified material. In a lengthy and detailed decision in 2003 examining this material, the New Zealand Refugee Status Appeals Authority found that that there were no serious reasons for considering that Zaoui was a member of a terrorist organisation or that he had committed the related crimes of which he had been convicted and granted him refugee status.[65]

AGREED HYPOTHETICAL CASE

A further alternative way in which arguments about the legality of international intelligence cooperation can be tested before courts without requiring full disclosure of sensitive facts on the government's behalf is for the parties to agree a hypothetical scenario which raises the relevant legal questions and allows the court to give a legal opinion. Although this procedure is not appropriate where a claimant is seeking a factual determination and a specific personal remedy, it can be useful where the dispute is fundamentally one of constitutional interpretation or administrative legality. In cases, for example, concerning the legality of international intelligence cooperation in relation to surveillance, there can be a legitimate reason for the government neither to confirm nor deny that cooperation with a foreign intelligence service has taken place. Equally, it would be unrealistic to expect the claimant to be able to discharge the burden of proving that it has. In a situation like this, an agreed hypothetical case allows for the relevant legal arguments nonetheless to be determined and for a binding pronouncement of legal principle to be made by the court. This procedure was adopted by the UK Investigatory Powers Tribunal in dealing with the claim brought by Privacy International and other NGOs that the alleged involvement of GCHQ in the PRISM and TEMPORA programmes was unlawful.[66]

ASSESSING THE EFFECT OF DISCLOSURE

One final option that deserves mention is where a domestic court is prepared to evaluate the impact of refusal to disclose international intelligence and, where the public interest so requires, to override the need to protect the information from disclosure. Naturally, courts should be wary of substituting their own assessment for that of the executive in this field. Nonetheless, exceptional cases can arise which show that secrecy should not be absolute. In the Binyam Mohammed case from the UK (Box 8.6), the Court of Appeal acknowledged the importance of the "originator control" principle (third party rule) with the implication that it would normally be upheld, but found that it could nevertheless be outweighed in exceptional circumstances, when reports of the applicant's mistreatment amounting to torture had been accepted in the partner state's own courts. The litigation is also important because of the court's insistence that it would not weigh the claim for non-disclosure unless it was properly supported by evidence from named foreign officials concerning the supposed harm that would follow to international relations if disclosure were ordered. The approach adopted by the UK courts in this instance has several advantages:

1. it allows for some (minimal) evaluation by the court of the veracity of the claim;
2. it allows for public discussion of the benefits of intelligence cooperation weighed against the impact on human rights, including the right to fair trial; and
3. by publicising and attributing claims for non-disclosure, it allows oversight bodies to hold intelligence services accountable for making these claims.

Box 8.6: The Binyam Mohammed case

The litigation was brought by the former Guantanamo Bay detainee Binyam Mohammed to force the UK Foreign Secretary to disclose potentially exculpatory material concerning his alleged torture in Pakistan. He had also been rendered by the US to Morocco and tortured there. The High Court initially decided to accede to the Foreign Secretary's request to maintain passages redacted from earlier judgments in the face of threats from the US to re-evaluate its intelligence sharing with the UK if the details based on reports from the US government to MI5 and MI6 about Binyam Mohammed's treatment were published.[67] The court later revisited its conclusion in the light of new information that became available, deciding in October 2009 that the public interest in discussion of allegations of complicity in torture outweighed the objections of the US authorities.[68]

This position was upheld in part by the Court of Appeal in February 2010 when the critical paragraphs were finally released.[69] By the time of this judgment, however, the US courts had found that Binyam Mohammed had been tortured, and the documents in question were in the public domain in the US. In effect, the Foreign Secretary's continued claim for non-disclosure was therefore simply to defend the principle of originator control, so that the US would have confidence that the UK authorities had taken all possible steps. It had been conceded that no remaining confidential information was at stake because of the US disclosure. The Court of Appeal recognised the importance of the control principle but held that in exceptional circumstances that could be outweighed by the public interest in disclosure.

The following recommendations are aimed at securing a fair trial where courts deal with cases involving international intelligence cooperation. It is stressed that these are not solely the responsibility of judges: they also require action by the executive as regards policy and practice and legislators in creating an appropriate legal framework for the courts to handle such cases.

Recommendations:

- Where legal measures (such as immigration or anti-terrorism measures) affecting individuals are based on international intelligence cooperation, the foreign intelligence service should be asked if it is possible for caveats to be relaxed or for the relevant intelligence to be summarised for use in legal proceedings
- Evidential safeguards for receiving international intelligence cooperation in legal proceedings should ensure that the court is able to order disclosure where the interests of justice so require, regardless of the provenance of the information concerned.
- In cases where the government instigates the litigation, preference should be given to not bringing or discontinuing litigation where non- or limited disclosure of information derived from or relating to international intelligence cooperation would undermine the other party's right to a fair trial.
- In cases of claims brought against the government instigated by the other party to which a claim for non-disclosure to protect international intelligence cooperation would apply, consideration should be given to the use of an agreed hypothetical case to allow for a determination by a court of the relevant legal questions. A court should not, however, sanction use of this process where a challenge relates to serious alleged violations of human rights.
- In dealing with claims for privilege or non-disclosure of information derived from or about international intelligence cooperation, courts should require specific claims of damage to international intelligence cooperation from the partner intelligence service as evidence, supported where appropriate by evidence from identifiable officials. In some instances, this may need to be heard by the judge *in camera* since the explanation may be exceptionally sensitive in relation to ongoing operations or intelligence sources and methods. The ultimate decision on, if, and how such information may be used must rest with a court.

8.7 International courts and tribunals and international intelligence cooperation

International courts and tribunals deal with questions of international intelligence cooperation in several different contexts. Complaints of violations of international human rights law arising from the activities of security and intelligence services may be made by individuals. Where a state is complicit in the action of foreign agents on its soil, such as facilitating or allowing them to detain and torture individuals or permitting them to abduct and transfer terrorist suspects without legal process,[70] its own responsibility under human rights law will be engaged. Equally, in some circumstances, when state officials are involved in actions outside their borders, state responsibility may apply under principles of extra-territoriality, depending on the degree of control they exercise.[71] In addition, the International Criminal Court and the special war crimes tribunals deal with allegations of violations of international criminal law where security and intelligence services of different states may be involved in various forms of cooperation to assist in tracing and apprehending state officials to bring them to trial in these courts.[72]

Some of the states most frequently cited in relation to recent abuse concerning

intelligence services are not party to the European Convention on Human Rights of 1950 nor subject to a regional court that engages in similar scrutiny, and do not recognise the jurisdiction of the International Criminal Court. For these reasons, some of the principles that international tribunals have developed that result in responsibility of member states, who are cooperation partners with states who are non-members (mentioned above and discussed further in Chapter 4), are especially significant. The *non-refoulement* principle prevents states from handing over a victim of persecution to persecution in another state. This is especially relevant to international intelligence cooperation in forbidding some forms of state involvement in rendition. As the European Court of Human Rights (ECtHR) has stated, in a case in which it found that Russian state agents had abducted the claimant (whose extradition been sought from Russia by Uzbekistan) and rendered him to Tajikistan: "any extra-judicial transfer or extraordinary rendition, by its deliberate circumvention of due process, is an absolute negation of the rule of law and the values protected by the Convention," and is "a violation of the most basic rights guaranteed by the Convention."[73]

The effect of these principles is discussed further in Chapter 4. The account here focuses on procedural aspects of human rights protection by international courts that are relevant to international intelligence cooperation. The ECtHR in particular has also adopted several practices designed to assist claimants who have difficulty in establishing the facts in the face of state silence and refusal to confirm or deny facts on grounds of national security.

Firstly, since the famous *Klass* case in 1978,[74] the ECtHR has recognized that some petitioners, such as those who may have been subject to secret surveillance, will face special difficulties in establishing a violation of their rights, and that there is a risk without a generous approach to who is regarded as a "victim," that effective protection would be undermined. The Court stated:

> An individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him. The relevant conditions are to be determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures.[75]

Many people about whom intelligence may have been exchanged between partner intelligence services will be unaware of the fact and in any event be unable to satisfy legal standards of proof. The Klass approach allows their cases to be heard if they satisfy the conditions outlined.

Secondly, the ECtHR has repeatedly held that a procedural obligation to investigate arises where credible allegations are made that an individual's right to life has been breached[76] and there is a similar procedural duty to investigate allegations of torture, ill treatment and undisclosed detention.[77] Where national authorities have conducted no effective investigation into actions involving human rights abuses at the hands of intelligence services and their international partners, the European Court of Human Rights has been prepared to find a breach of European Convention on Human Rights (see the decision in *El-Masri v FYR Macedonia*, Box 8.7 below).

Box 8.7: State complicity for rendition before the European Court of Human Rights

On 13 December 2012, the Grand Chamber of the European Court of Human Rights issued its ruling on the CIA's detention and rendition of Khaled El-Masri, holding a European state accountable for its involvement in the secret US-led programmes for the first time. The European Court of Human Rights held unanimously that the former Yugoslav Republic of Macedonia was responsible for German national Khaled El-Masri's unlawful detention, enforced disappearance, torture and other ill-treatment, and for his transfer out of Macedonia to locations where he suffered further serious violations of his human rights. It further held that Macedonia had not satisfied its obligation to carry out an effective investigation. Khaled El Masri had been arrested on 31 December 2003 by Macedonian authorities and later handed over to CIA agents, who transferred him to a secret detention facility in Afghanistan, having mistaken him for a "terrorist" suspect, where he was held incommunicado and allegedly subjected to torture. On 28 May 2004, Khaled El-Masri was put on a plane and flown to Albania where he was released.[78]

Thirdly, in several cases involving "extraordinary rendition" by state agents, the Court has inferred state liability from the surrounding circumstances: noting the objective difficulties for an applicant in providing evidence in support of an allegation; that the events at issue lay within the exclusive knowledge of the authorities; that a forcible transfer to another state could not have happened without the knowledge and either passive or active involvement of the authorities; and the failure of the respondent state to provide a plausible explanation.[79]

The process of inference can be seen used strikingly in the case of Abd Al Rahim Hussayn Muhammad Al-Nashiri, who applied to the European Court Human Rights, alleging that he had been detained incommunicado and tortured at a secret prison run by the CIA on Polish territory and subjected to rendition in being removed to Morocco and then Guantanamo Bay, as part of the US High Value Detainees programme.[80] The Court acknowledged the difficulties involved in gathering and producing evidence caused by the restrictions on their communication with the outside world, the extreme secrecy surrounding the US rendition operations, and the Polish Government's failure to cooperate with the Court in its examination of the case. Despite these obstacles, the Court's undertook a thorough examination of the available material, based on circumstantial evidence, including a large amount of evidence obtained through international inquiries, redacted documents released by the CIA, other public sources, and evidence from experts and witnesses (see further Box 8.8). It also held an in camera fact-finding hearing, during which it heard evidence from three experts, Claudio Fava, former Member of the European Parliament and rapporteur of the Temporary Committee on the alleged use of European states by the CIA for the transport and illegal detention of prisoners; Swiss Senator Dick Marty; and Mr J.G.S., a lawyer and investigator; as well as from a witness, Senator Józef Pinior, former Member of the European Parliament and a member of the Polish Senate. It concluded that Poland had failed in its duty to assist the Court under Article 38 and was responsible for breaching the applicant's rights under Articles 3, 5, 6 and 8 of the European Convention.

Box 8.8: Inferring state responsibility: CIA "black sites" in Poland and the European Court of Human Rights

While it is for the applicant to make a *prima facie* case and adduce appropriate evidence, if the respondent Government in their response to his allegations fail to disclose crucial documents to enable the Court to establish the facts or otherwise provide a satisfactory and convincing explanation of how the events in question occurred, strong inferences can be drawn.

According to the Court's case-law [on the rights to life and not to be subjected to torture] where the events in issue lie wholly, or in large part, within the exclusive knowledge of the authorities… strong presumptions of fact will arise in respect of injuries and death occurring during that detention.

The burden of proof in such a case may be regarded as resting on the authorities to provide a satisfactory and convincing explanation and in its absence the Court can draw inferences which may be unfavourable.

Taking into consideration all the material in its possession the Court found:
(a) that Poland knew of the nature and purposes of the CIA's activities on its territory and that, by enabling the CIA to use its airspace and the airport, by its complicity …. Poland cooperated in the preparation and execution of the CIA rendition, secret detention and interrogation operations on its territory;
(b) that, given that knowledge and the emerging widespread public information about ill-treatment and abuse of detained terrorist suspects in the custody of the US authorities, Poland ought to have known that, by enabling the CIA to detain such persons on its territory, it was exposing them to a serious risk of treatment contrary to the Convention.[81]

Recommendation:

In situations of alleged international intelligence cooperation involving extraordinary rendition or forcible transfer, where only the state could offer an explanation and none is forthcoming, it may be appropriate for a court to infer knowledge and responsibility on the part of a state that is a partner to such action from other available credible evidence.

Endnotes

1. The extent of recourse to litigation varies, however, between states for a variety of factors.
2. Some states may use different models in their criminal and civil proceedings, as in the discussion of the Netherlands and the UK below.
3. See Italian Constitutional Court Judgment 106/2009. When the effect of that ruling was limited by the interpretation of the Supreme Court of Cassation to only cover legitimate intelligence actions (Cass., sez. V pen., judgment 46340/2012) and they were convicted by the Court of Appeal of Milan (Corte App., sez IV pen., judgment 985/2013), the Constitutional Court reaffirmed its earlier view (Judgment 24/2014) leading to their later acquittal (Cass., sez. I pen., judgment 20447/2014). See European Parliament's Committee on Civil Liberties Justice and Home Affairs, *National security and secret evidence in legislation and before the courts: exploring the challenges*, PE 509.991, Annex 5 (Country Fiche: Italy); Box 8.3 deals with the proceedings in the case brought against US officials.
4. *United States v. Reynolds*, 345 U.S. 1.
5. See *El- Masri v. Tene*t, 479 F.3d 296 (4th Cir. 2007), *cert. denied,* 128 S.Ct. 373 (2007); *Arar v. Ashcroft*, 414 F. Supp. 2d 250 (E.D.N.Y.2006); aff'd 2 November 2009 (2nd Cir, en banc); *Mohamed v. Jeppesen Dataplan, Inc.*, 539 F. Supp. 2d 1128, 1129 (N.D.Cal. 2008), aff'd, 614 F.3d 1070 (9th Cir. 2010) (en banc), cert. denied, 131 S. Ct. 2442 (2011). See generally: Timothy Bazzle, "Shutting the Courthouse Doors: Invoking State Secrets Privilege to Thwart Judicial Review in the Age of Terror," *Civil Rights Law Journal 23*, (2012): 23-71.
6. *Conway v. Rimmer* [1968] AC 910.
7. Section 99 Code of Administrative Procedure, introduced following the judgment of the Federal Constitutional Court, 27 October 1999, 1 BvR 385/90.
8. Administrative Division of the Council of State, 30 November 2011, LJN BU6382, AB 2012/142.
9. In the UK the so-called *Norwich Pharmacal* remedy, which takes its name from the case of *Norwich Pharmacal v. Commissioners of Customs and Excise* [1974] AC 133, allows a litigant to seek disclosure of evidence from third parties to litigation in this way.
10. Arts. 202 and 256 of the Italian Code of Criminal Procedure and Art. 41 of Law 124/2007.
11. European Parliament's Committee on Civil Liberties Justice and Home Affairs, *National security and secret evidence in legislation and before the courts*, 134-135.
12. Amendment to Article 187d CPC.
13. J.E.B. Coster van Voorhout, "Intelligence as Legal Evidence: Comparative Criminal Research into the Viability of the Proposed Dutch Scheme of Shielded Intelligence Witnesses in England and Wales, and Legislative Compliance with Article 6(3)(d)ECHR," *Utrecht Law Review* 2(2), (2006): 119-144; Q. Eijkman & B. van Ginkel, "Compatible or Incompatible? Intelligence and Human Rights in Terrorist Trials," *Amsterdam Law Forum* 3, (2011): 3-16.
14. Study for the European Parliament's Committee on Civil Liberties Justice and Home Affairs, *National security and secret evidence in legislation and before the courts*, 122-124.
15. For critical discussion of the 2013 Act, see A.Peto and A.Tyrie, *Neither Just Nor Secure*, Centre for Policy Studies, 2013; A.Tomkins, "Justice and security in the United Kingdom," *Israel Law Review*, (2013); T. Hickman, "Turning out the lights: the Justice and Security Act 2013," *UK Constitutional Law Association*, (2013).
16. Notes 11-15 above.
17. Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs and Human Rights (Rapporteur: Mr Dick Marty), *Abuse of state secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations*, Doc. 11907, 16 September 2011.
18. See further: 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); C. Murray, "Out of the Shadows: the Courts and the United Kingdom's Malfunctioning Counter-Terrorism Partnerships," *Journal of Conflict & Security Law* 18(2), (2013): 193-232.
19. In *Khadr v. Canada* [2008] SCC 28, the Supreme Court of Canada held that the Canadian Charter of Rights applied extraterritorially to interrogation conducted by officers of the Canadian Security Intelligence Service of an inmate held unlawfully by the US at Guantánamo Bay. In order to give effect to s. 7 of the Charter the Canadian Government was obliged to disclose transcripts of the interviews. For subsequent proceedings, see [2008] FC 807. For earlier related litigation, see *Khadr v. Canada (Minister of Foreign Affairs)*, [2004] FC 1393; *Khadr v. Canada* [2005] FC 1076, [2006] 2 F.C.R. 506; (2005) 257 D.L.R. (4th) 577.
20. In *Wakeling v. United States of America* [2014] SCC 72 the Supreme Court of Canada held that the disclosure of intercept material from the Canadian to the US authorities (in a drugs investigation) was governed by the Canadian Charter of Rights and

(on the facts) had a lawful basis. However the SCC considered that the use of protocols, caveats, or agreements may be relevant to assessing whether such a disclosure was carried out in a reasonable manner. It remarked that information sharing protocols or caveats would be insufficient to mitigate the risk where the disclosing party 'knows or should have known that the information could be used in unfair trials, to facilitate discrimination or political intimidation, or to commit torture or other human rights violations' and that in such cases the Charter of Rights would forbid disclosure.

21. *Equality and Human Rights Commission v. Prime Minister* [2011] EWHC 2401 (Admin), [2012] 1 WLR 1389 (unsuccessful challenge to legality of guidance issued by the Prime Minister to guide UK intelligence officials in questioning detainees abroad held by partners where ill-treatment may have occurred).
22. *R (application of Khan) v. Secretary of State for Foreign and Commonwealth Affairs* [2014] All ER (D) 112 (Jan); [2014] EWCA Civ 24 (legality of alleged passing by GCHQ to the US of locational information to CIA for drone attacks in Pakistan unsuccessfully challenged because the court refused to make a declaration that would involve judging the acts of a sovereign foreign government (the USA) and because of the hypothetical nature of the alleged criminality involving GCHQ officials).
23. "Court dismisses claim of German complicity in Yemeni drone killings," *The Guardian*, 27 May 2015.
24. For example: *El- Masri v. Tenet*, 479 F.3d 296 (4th Cir. 2007); *Arar v. Ashcroft*, 414 F. Supp. 2d 250 (E.D.N.Y.2006).
25. See Box 8.3 concerning the Abu Omar case. Prosecutors in Lithuania have reportedly opened investigations into allegations of concerning the unlawful detention of Mustafa al-Hawsawi, at a CIA detention facility in the country: "Lithuania opens probe into CIA 'black site' allegations," *EU Business*, 20 February 2014.
26. Note 2 above. In Germany there is controversy that data sent by the BND to NSA could have been used for targeting German citizens in Afghanistan by drones: "Germany denies phone data sent to NSA used in drone attacks," *The Guardian*, 12 August 2013.
27. *General Prosecutor at the Court of Appeals of Milan v. Adler and ors*, Final appeal judgment, No 46340/2012; ILDC 1960 (IT 2012), 29 November 2012.
28. The convictions of the former head of the Italian military secret services, Nicolò Pollari, of his deputy, Marco Mancini, and of other three Italian secret agents for their alleged complicity in the unlawful rendition on the basis that their acts were covered by the secret of state doctrine (see note 3 above).
29. See *General Prosecutor at the Court of Appeals of Milan v. Adler and ors*, First instance judgment, Tribunal of Milan, Fourth Criminal Section, No 12428/09; ILDC 1492 (IT 2010), 4 November 2009.
30. *General Prosecutor at the Court of Appeals of Milan v. Adler and ors*, Final appeal judgment.
31. On 5 April 2013, the President of the Italian Republic, Giorgio Napolitano, granted a pardon for US Colonel Joseph L. Romano III.
32. (24 April 1963) 596 UNTS 261; 21 UST 77; TIAS No 6820, entered into force 19 March 1967.
33. See note 3 above.
34. The Special Immigration Appeals Commission (SIAC) was established to bring the procedure into conformity with Article 6 following the European Court of Human Rights adverse ruling in *Chahal v. United Kingdom* (1996) 23 EHRR 413; *A. and Others v. The United Kingdom*, no. 3455/05, Judgment, 19 Feb. 2009.
35. In the UK: *R v. Mullen* [1999] 2 Cr App R 143 (treating 'rendition to justice' in cooperation with agents of a foreign state as an abuse of process, resulting in the prosecution being struck out); *R v. Horseferry Magistrates Court, ex p. Bennett* [1994] 1 AC 42.
36. For example, in 2005 the United States refused to allow the presentation of intelligence evidence in the trial in Germany of Abdelgheni Mzoudi for allegedly aiding the 9/11 plotters- resulting in his acquittal. Likewise, in the Lappass prosecution in Australia in 2003 the sensitivities of an (unnamed) country whose documents had been disclosed by an official led to consideration of security vetting of defence counsel as a pre-condition of further disclosure of the documents.
37. *R (Corner House Research) v. Director of the Serious Fraud Office* [2008] UKHL 60.
38. See: UK, *R (Al Rawi and others) v. Secretary of State for Foreign and Commonwealth Affairs and Secretary of State for the Home Department* (United Nations High Commissioner for Refugees intervening) [2006] EWCA Civ 1279, 12 October 2006 (unsuccessful challenge brought by two UK residents who had been taken to Guantanamo Bay from Gambia, via Afghanistan, following apparent collusion between the UK, Gambian and US authorities); Australia, *Hicks v. Ruddock* [2007] 156 FCR 574; [2007] FCA 299, 8 March 2007.(unsuccessful challenge by an Australian captured by Alliance forces in Afghanistan in November 2001 and taken to Guantanamo Bay to

the refusal of the Australian government to make diplomatic representations on his behalf). See N. Klein and L.Barry, "A Human Rights Perspective on Diplomatic Protection: David Hicks and his dual nationality," *Australian Journal of Human Rights* 1, (2007): 13.

39. For example the UK decision in *A (No 2) v. Secretary of State for the Home Department* [2005] UKHL 71. The majority ruled that the evidence would only be inadmissible if on the balance of probabilities the evidence had been obtained by torture. The minority argued that the evidence must be excluded if there was a real risk that the evidence had been obtained by torture. See further Ch. 4.
40. Intelligence partners may give evidence of harm in the proceedings.
41. See Section 8.5 below.
42. Ian Leigh, "The Role of Judges" in *Commissions of Inquiry and National Security: Comparative Approaches*, ed., S. Farson and M.Pythian, (Praeger, 2010), ch. 16.
43. 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*, (Ottawa: Canadian Government Publishing, 2006); Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Factual Background Volume II*, (Ottawa: Canadian Government Publishing, 2006); See further A. Wright, "Fit for Purpose? Accountability challenges and paradoxes of domestic inquiries," in *International Intelligence Cooperation and Accountability*; A subsequent inquiry that operated wholly in camera was conducted by former Federal Court of Canada Chief Justice Iacobucci into the cases of Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin; The Honourable Frank Iacobucci, QC, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin*, (Ottawa: Canadian Government Publishing, 2010).
44. *Arar Report: Analysis and Recommendations*, 339-42, discussing proposals for tightening the use of caveats in exchange of intelligence.
45. *Arar Report: Analysis and Recommendations and Factual Background*.
46. *Arar Report: Analysis and Recommendations*, 344.
47. See section 8.1 above.
48. A senior United Kingdom judge, Lord Hoffmann, explained "…in matters of national security, the cost of failure can be high. This seems to me to underline the need for the judicial arm of government to respect the decisions of ministers of the Crown on the question of whether support for terrorist activities in a foreign country constitutes a threat to national security. It is not only that the executive has access to special information and expertise in these matters…" (*Secretary of State for the Home Department v. Rehman* [2001] UK HL 47; [2002] 1 All ER 122, para. 62.)
49. Note 22 above. In 2013 the German Federal Prosecutor General decided to discontinue investigation into the killing of a German national in a drone strike in Pakistan since the suspects, who were CIA operatives, would enjoy immunity from prosecution if there had been no violation of international humanitarian law; The International Court of Justice has confirmed the existence of state immunity before municipal courts as a matter of international law and rejected the suggestion: International Court of Justice, Reports of Judgments, Advisory Opinions and Orders, *Jurisdictional Immunities of the State (Germany v. Italy; Greece intervening*), Judgment of 3 February 2012; The European Court of Human Rights has found that the operation of state immunity to prevent actions by UK nationals for alleged abduction and torture by foreign officials does not constitute a violation of Article 6: *Al-Adsani v. United Kingdom* (2002) 34 EHRR 11. See also *Jones v. UK*, nos. 34356/06 and 40528/06), ECtHR, 14 January 2014 and *Stichting Mothers of Srebenica v. Netherlands*, no. 65542/12, ECtHR, 11 June 2013.
50. *Belhaj v. Straw and others* [2014] EWCA Civ 1394. The decision is on appeal to the UK Supreme Court.
51. See further: Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs and Human Rights (Rapporteur: Mr Dick Marty), *Abuse of state secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations*, Doc. 11907, 16 September 2011; European Parliament's Committee on Civil Liberties Justice and Home Affairs, *National security and secret evidence in legislation and before the courts*.
52. *Tinnelly and McElduff v. UK*, ECtHR, (1999) 27 EHRR 249; *Rowe and Davis v. UK*, ECtHR, (2000) 30 EHRR 1; *Edwards and Lewis v. UK*, ECtHR, 27 October 2004.
53. British–US Communication Intelligence Agreement, 5 March 1946.
54. New Zealand, Official Information Act, 1982 s. 31; Australia, Freedom of Information Act 1982, s.33(4) and s. 55 (5A).

55. Access to Information Act s. 69.1, inserted by the Anti-Terrorism Act 2001. See: P. McMahon, "Special Notes On Bill C-36: Amending the Access to Information Act: Does National Security Require the Proposed Amendments of Bill C-36?" *University of Toronto Faculty of Law Review 60*; R. Daniels, P. Macklem and K. Roach, *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*, (Toronto: University of Toronto Press, 2001).
56. s. 58B(2) Freedom of Information Act 1982. R. Snell, "Conclusive or Ministerial Certificates: An Almost Invisible Blight in FOI Practice," *Freedom of Information Rev. 9*, (2004): 109.
57. In 2006 in *McKinnon v. Secretary, Department of Transport* [2006] HCA 45; (2006) 229 ALR 187; the High Court of Australia gave its first ruling on the standard to be applied by the AAT in considering conclusive certificates. Although the case did not involve disclosure of intelligence material it nevertheless sheds light on the process to be applied. The High Court upheld the procedure adopted by the AAT of inspecting all the documents in contention (these concerned economic policy at senior and ministerial level in the Treasury), hearing witnesses from each side (who were cross-examined), hearing some in camera evidence, and determining firstly whether there were rational and permissible grounds for the claim and, secondly, whether there was a substantial factual basis for concluding that the documents fell within those grounds. The judgment appears to endorse a responsible and measured way for probing sensitive secrecy claims.
58. Bundesverfassungsgeright [Federal Constitutional Court of Germany], 2 BvE 3/07.
59. *Charkaoui v. Canada* (Citizenship and Immigration), [2008] 2 S.C.R. 326, 2008 SCC 38.
60. See section 8.1 above and *Al Rawi and others v. Security Service* [2011] UKSC 34.
61. See UK, Secretary of State for Justice, *Response to the public consultation on Justice and Security*, (London, 2012); Liberty, *Liberty's Response to the Ministry of Justice's Consultation 'Judicial review: proposals for further reform*, (London, 2013); Human Rights Joint Committee, 24th Report for 2011-12, *The Justice and Security Green Paper*, HL 286/ HC 1777 (2011-12).
62. See also Box 3.4.
63. 'Summary of Allegations' and reasoning of the Director of Security in making a Security Risk Certificate about Mr Ahmed Zaoui, released by Ahmed Zaoui's lawyers on 20 Feb 2004.
64. By a decision of the Federal Council of 27 April 1998; Zaoui complained unsuccessfully to the European Court of Human Rights that these restrictions violated his rights under Arts. 9 and 10 ECHR: *Zaoui v. Switzerland* Application no. 41615/98, 18 January 2001, declared inadmissible.
65. Refugee Appl. 74540, 1 August 2003.
66. *Liberty and others v. The Secretary of State for Foreign and Commonwealth Affairs and others*, nos. IPT/13/77/CH; 13/92/CH; 13/194/C and 13/204/CH, [2015] UKIPTrib 13_77–H.
67. *R (Binyam Mohammed) v. Secretary of State for Foreign and Commonwealth Affairs* [2009] EWHC 152 (Admin).
68. *R (Binyam Mohammed) v. Secretary of State for Foreign and Commonwealth Affairs* (No. 5) [2009] EWHC 2549 (Admin).
69. *R (Binyam Mohammed) v. Secretary of State for Foreign and Commonwealth Affairs* [2010] EWCA Civ 65.
70. See the following decisions of the European Court of Human Rights: *El-Masri v. the former Yugoslav Republic of Macedonia*, no. 39630/09, 13 December 2012; *Al Nashiri v. Poland* no. 28761/11, 24 July 2014; *Husayn (Abu Zubaydah) v. Poland*, no. 7511/13, 24 July 2014.
71. See *Al-Skeini and Others v. UK*, no. 55721/07, ECtHR (Grand Chamber), 7 July 2011, paras. 134-136; *Al-Saadoon and Mufdhi v. UK*, no. 61498/08, ECtHR, 2 March 2010 (finding that the UK breached Art. 3 ECHR by transferring applicants from military custody to Iraqi authorities to face trial where they were liable to the death penalty); *Hirsi Jamaa v. Italy,* no. 27765/09, ECtHR (Grand Chamber), 23 February 2012 (violation arising from interception of immigrants, transfer onto Italian military vessels and return to Libya pursuant to bi-lateral agreement between Italy and Libya); *M v. Denmark* no. 17392/90, ECommHR, 14 October 1992 (admissibility) (arising from the invitation by the Danish ambassador to East German police to enter the Danish embassy to arrest the applicant).
72. Consequently, questions about the legality of the cooperation and of related evidence may arise in war crimes trials. In particular note: *Prosecutor v. Tihomir Blaskic (Judgement on the Request of the Republic of Croatia for Review of the Decision of Trial Chamber II of 18 July 1997)*, ICTY Appeals Chamber, 29 October 1997, no. IT-95-14, para. 68; *Prosecutor v. Tihomir Blaskic (Judgement)*, ICTY Appeals Chamber, 29 July 2004, no. IT-95-14; For discussion, see S.Chesterman, "Intelligence Cooperation in international operations: peacekeeping, weapons inspections, and the apprehension and prosecution of war criminals," in *International Intelligence Cooperation and Accountability*, 138-141.

73. *Abdulkhakov v. Russia*, no. 14743/11, ECtHR, 2 October 2012, para. 165. See also *Savridden Dzhurayev v. Russia*, no. 71386/10, ECtHR 25 April 2013; *Koziyev v. Russia*, no. 58221/10; *Zokhidov v. Russia*, no. 67286/10; *Iskandarov v. Russia*, no. 17185/05, 23 September 2010.
74. *Klass v. Germany* (1979-80) 2 EHRR 214.
75. Ibid., para. 34
76. For example: *Edwards v. The United Kingdom*, no. 46477/99, para. 69; *Varnava and Others v. Turkey*, no. 16064/90, para 191.
77. For example, *Al Nashiri v. Poland*, no. 28761/11, 24 July 2014.
78. *El-Masri v. FYR Macedonia*, no. 39630/09, 13 December 2012.
79. Ibid.; *Abdulkhakov v. Russia*, no. 14743/11, ECtHR, 2 October 2012, para. 165; See also *Savridden Dzhurayev v. Russia*, no. 71386/10, ECtHR 25 April 2013; *Koziyev v. Russia*, no. 58221/10; *Zokhidov v. Russia*, no. 67286/10; *Iskandarov v. Russia*, no. 17185/05, 23 September 2010.
80. *Al Nashiri v. Poland*, no. 28761/11, 24 July 2014. See also the parallel case of *Husayn (Abu Zubaydah) v. Poland*, no. 7511/13, 24 July 2014.
81. *Al Nashiri v. Poland*, no. 7511/13, Judgment of 24 July 2014, Paras. 395-396, 442.

Recommendations

CHAPTER 4

- Before entering bilateral or multilateral agreements for international intelligence cooperation, states should carefully review their compatibility with the state's international legal obligations.
- All agreements for international intelligence cooperation should explicitly state that the parties' international legal obligations take priority over them.
- All officers of intelligence services, whose duties involve international intelligence cooperation, should receive training in the international law implications of their work.
- Intelligence services should have ready access to specialist legal advisers familiar both with these obligations and with general principles of international law.
- An intelligence service should be legally obliged to use due diligence to determine that outgoing information will not be used by a partner service to assist or contribute towards violations of international human rights law, at the very least by conducting a risk assessment
- An intelligence service should be legally obliged to use due diligence to determine that incoming information has not been obtained as a result of torture, at the very least by conducting a risk assessment.
- A state that hosts intelligence facilities of a partner state or permits a partner intelligence service to operate in its territory should ensure that the arrangements for doing so allow it to fully discharge its own obligations under international human rights law.

CHAPTER 5

- The legislative mandate of each of the intelligence services should specify the general purposes for which intelligence can be lawfully be gathered and used (regardless of whether accessed through cooperation or other methods), the method by which it can be accessed and the main conditions to be met where the executive authorise cooperation.
- Legislation should prohibit intelligence services from using 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.
- Freedom of information or official secrets legislation should only prevent disclosure of information concerning international intelligence cooperation if the public interest in non-disclosure outweighs that in disclosure.
- Legislation should provide for the procedure for approval of international intelligence cooperation agreements by the executive (for example, by a specified minister responsible for the intelligence service).

- Procedural requirements should also include consideration of the human rights record of intelligence services with which information exchanged, so that appropriate safeguards can be put in place if necessary.
- The legislative mandates of bodies that oversee the intelligence services (including parliamentary committees, non-parliamentary expert bodies, and, where their mandate includes the services, data protection and information commissioners, ombuds institutions and human rights commissions) should make clear that their role and powers extend to relevant intelligence cooperation and activities of the services they oversee.
- Legislation should include provisions that oblige the service and/or executive to inform the intelligence oversight body about international intelligence cooperation agreements.
- Legislation should include provisions on the duty of record keeping for international intelligence cooperation, in particular, concerning the exchange of information with foreign partners.
- Legislation should govern the supply by an intelligence service of information containing personal data to a foreign service. The legislation should prescribe when and what information may be shared in a manner consistent with the state's human rights obligations (i.e. for legitimate aims and only where necessary and proportionate to those aims).
- Legislation should govern the receipt by an intelligence service of information containing personal data from a foreign service. The legislation should prescribe when and what information may be retained, destroyed, processed, or disseminated in a manner consistent with the state's human rights obligations (i.e. for legitimate aims and only where necessary and proportionate to those aims).
- Legislation should make it clear if services utilise liaison/international intelligence cooperation to gather information about persons within their jurisdiction, then they should be required to meet the same requirements as would apply when seeking that information themselves (i.e. concerning permissible purpose, threshold of suspicion, and independent authorisation).
- In particular, where bulk material is transferred by a foreign intelligence or signals intelligence agency, the recipient agency should only be permitted by legislation to search it if all the material requirements of a national search are fulfilled and this is authorized, in the same way as a search of bulk material directly obtained by the recipient agency itself.

CHAPTER 6

- Intelligence service managers should put in place risk assessment processes for international intelligence cooperation that set out the factors which must be considered before undertaking particular types of cooperation. These processes adopted should take account of an intelligence service's domestic and international legal obligations.
- Oversight bodies should verify that such processes exist and evaluate risk assessment policies and practices to satisfy themselves that relevant factors are considered.
- The executive should ensure that there is cross-government sharing of appropriate information on countries' human rights records as this assists services in undertaking risk assessments.

- Oversight bodies should examine whether intelligence services' risk assessment processes take account of information from reputable NGOs and international organisations.
- Oversight bodies should review intelligence service decisions to request information from foreign services with poor human rights records. They should also examine policies and procedures for assessing the reliability of and recording/marking incoming information received from such services.
- Intelligence services should ensure that caveats are attached to information shared with foreign partners.
- Caveats should set out in unambiguous terms the use to which that information may be put and with whom it may be shared.
- Oversight bodies should review the standard caveats attached to outgoing information as well as intelligence service policies for monitoring adherence to caveats and addressing breaches of caveats by foreign services.
- Reliability assessments should be attached to intelligence shared with foreign partners, particularly where it relates to identifiable individuals.
- Overseers should pay close attention to the use of assurances in situations where there exists a risk that outgoing information could be used in violation of human rights. Overseers should examine:
  - whether assurances are sought,
  - whether they are sufficiently detailed and credible,
  - whether it is reasonable to reply on them, and
  - whether mechanisms exist for ensuring that they are being adhered to.
- Intelligence service personnel involved in international intelligence cooperation should be provided with training on the risks involved, including how to identify, report, and mitigate risks to human rights. Training should also include guidance on requirements for seeking authorisation from senior management and/or the executive, record keeping, and service obligations to external oversight bodies.
- Overseers should evaluate services' training programmes and satisfy themselves that training on relevant aspects of international intelligence is not only is provided but is also understood by intelligence officers.
- There should be clear requirements on the recording of cooperation with foreign services. These should include requests made/received and information sent to/received from foreign services, as well as on internal decision making relating to international intelligence cooperation.
- Intelligence services should be required by law to establish internal mechanisms through which their staff can disclose information or concerns relating to wrongdoing by a foreign partner or colleagues within their own service.
- Intelligence service personnel should be permitted to make protected disclosures relating to international intelligence cooperation (or any other matters) to an external oversight body, which is required to investigate disclosures of information showing wrongdoing.
- Governments should ensure that procedures and protections for intelligence service personnel wishing to disclose concerns comply with the minimum standards set out in the Global Principles on National Security and the Right to Information.

- Ministers responsible for intelligence services should ensure that they have access to dedicated (non-intelligence service) staff who can advise them on decisions relating to the intelligence services.
- Ministers should ensure that training on intelligence (including international intelligence cooperation) is given to the officials responsible for advising/assisting them in this area.
- Ministers should require intelligence service heads to keep them apprised of relevant developments in their relationships with foreign services. They should use meetings/briefings with service heads to enquire about international intelligence cooperation-related matters.
- Oversight bodies should verify whether there are ministerial guidelines in place that govern international intelligence cooperation.
- Oversight bodies should identify areas of international intelligence cooperation decision making in which an intelligence service would benefit from ministerial direction.
- Services or the executive should consider publishing ministerial directives on international intelligence cooperation in order to promote discussion on such policies and to increase public confidence in the intelligence services.
- Ministerial or intelligence service guidelines should make clear which types of international intelligence cooperation-related decisions require consultation with and/or the approval of ministers. Overseers should evaluate whether such guidelines require appropriate decisions to be referred to ministers and whether the guidelines are followed in practice.
- The law should require that the executive approves any new or significantly-amended agreement or memorandum of understanding between an intelligence service and a foreign entity.

CHAPTER 7

- Consideration should be given to providing external oversight bodies an explicit legal mandate to scrutinise international intelligence cooperation. Regardless of whether their mandate refers to international intelligence cooperation, oversight bodies should (if they have not done so already) monitor their services' cooperation with foreign partners.
- There should be at least one external oversight body that is empowered to scrutinise the policies the practices relating to both the outgoing and incoming sharing of personal data with foreign entities.
- Overseers responsible for scrutinising intelligence budgets should examine the allocation and use of financial resources for international intelligence cooperation, including for providing equipment and training to foreign entities and joint surveillance infrastructure.
- An external oversight body should evaluate executive involvement in international intelligence cooperation to assess whether it is sufficient and consistent.
- External overseers should evaluate the adequacy of processes used to keep the executive informed about intelligence service cooperation with foreign entities.

- External overseers should examine whether there are ministerial directives relating to international intelligence cooperation, ensure that any directives are consistent with the legislation, and highlight areas in which further ministerial guidance may be beneficial.
- Oversight bodies should identify aspects of their services' cooperation with foreign entities to be monitored on a periodic basis.
- Legislation should empower oversight bodies to undertake investigations on their own-initiative and overseers should use these powers to carry out thematic investigations into intelligence services' policies and practices relating to international intelligence cooperation.
- There should be at least one external oversight body that has full access to information held by the intelligence services, including information from or pertaining to international intelligence cooperation, which it considers to be relevant to the fulfilment of its mandate.
- The third party rule or control principle should not be permitted to override statutory provisions granting oversight bodies access to information necessary to fulfil their mandates. Parliamentarians should consider making it explicit in legislation that oversight bodies' access to information is not constrained by or subject to the third party rule.
- Consideration should be given to requiring intelligence services to include in their agreements with foreign partners a clause stating that cooperation may be subject to scrutiny by a particular oversight body.
- Legislation should empower oversight bodies to hire security-cleared technological experts to assist them in understanding and assessing complex systems for the purposes of their oversight.
- Additional resources should be allocated to oversight bodies to enable them to engage staff or external experts to assist them in understanding complex technology used by intelligence services, including in their cooperation with foreign partners.
- Consideration should be given to making general information about international intelligence cooperation public, including relevant ministerial directions or guidelines and oversight bodies' reports on international intelligence cooperation.
- Overseers should encourage the executive and services to improve transparency in relations to international intelligence cooperation.
- Oversight bodies in states whose intelligence services cooperate with each other should work with their foreign counterparts to consider the possibility of developing processes for:
  a. alerting each other to areas of mutual concern in the of the cooperation between their services, and
  b. requesting that their foreign counterpart investigate and provide unclassified reports on specific issues of mutual concern that arise on the counterpart's side of an international intelligence cooperation relationship.
- Consideration should be given to providing oversight bodies with additional staff and resources to enable them to continue to provide advice and support to oversight bodies in emerging democracies. Such staff could also facilitate additional cooperation with well-established foreign counterparts.

CHAPTER 8

- Legislators and courts should devise processes by which intelligence can be handled securely in litigation while also protecting the right to fair trial as much as possible. Such legislation or procedures should guarantee that restrictions only apply where strictly necessary, and that the final decision on disclosure is made by a court.
- Any procedure adopted to protect classified information or intelligence cooperation relationships in litigation should not prevent access by a victim of human rights to an effective remedy or allow for suppression of information concerning gross human rights violations.
- Where legal measures (such as immigration or anti-terrorism measures) affecting individuals are based on international intelligence cooperation, the foreign intelligence service should be asked if it is possible for caveats to be relaxed or for the relevant intelligence to be summarised for use in legal proceedings
- Evidential safeguards for receiving international intelligence cooperation in legal proceedings should ensure that the court is able to order disclosure where the interests of justice so require, regardless of the provenance of the information concerned.
- In cases where the government instigates the litigation, preference should be given to not bringing or discontinuing litigation where non- or limited disclosure of information derived from or relating to international intelligence cooperation would undermine the other party's right to a fair trial.
- In cases of claims brought against the government instigated by the other party to which a claim for non-disclosure to protect international intelligence cooperation would apply, consideration should be given to the use of an agreed hypothetical case to allow for a determination by a court of the relevant legal questions. A court should not, however, sanction use of this process where a challenge relates to serious alleged violations of human rights.
- In dealing with claims for privilege or non-disclosure of information derived from or about international intelligence cooperation, courts should require specific claims of damage to international intelligence cooperation from the partner intelligence service as evidence, supported where appropriate by evidence from identifiable officials. In some instances, this may need to be heard by the judge in camera since the explanation may be exceptionally sensitive in relation to ongoing operations or intelligence sources and methods. The ultimate decision on, if, and how such information may be used must rest with a court.
- In situations of alleged international intelligence cooperation involving extraordinary rendition or forcible transfer, where only the state could offer an explanation and none is forthcoming, it may be appropriate for a court to infer knowledge and responsibility on the part of a state that is a partner to such action from other available credible evidence.

Author Biographies

HANS BORN is Deputy Head Research at the Geneva Centre for Democratic Control of Armed Forces (DCAF). He currently focuses on the role of parliaments and ombuds-institutions in security sector governance as well as police accountability and democratic oversight of intelligence services. His regional specialization is Southeast Asia where he leads regional and in-country programmes aimed at strengthening democratic governance of the security sector (including in Cambodia, Indonesia, Myanmar, 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 PhD in social sciences from Tilburg University (the Netherlands).

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 on matters related to human rights and security sector reform to the OSCE Office of Democratic Institutions and Human Rights, to the Council of Europe, to the EU Fundamental Rights Agency and to the UNDP.

AIDAN WILLS is a consultant on security sector governance and human rights. He has published widely on the oversight of security services and police, access to information in the national security field and whistleblowing. His publications include *International Intelligence Cooperation and Accountability* (with H Born and I Leigh - 2011), *Parliamentary Oversight of Security Agencies in EU* (with M Vermeulen - 2012) and *Democratic and Effective Oversight of National Security Services* (2015). Aidan was heavily involved in drafting both the *Global Principles on National Security and the Right to Information*,

and the *UN compilation on intelligence agencies and their ovesight*. He has acted as a consultant to the UN Special Rapporteur on counter-terrorism and human rights, the European Parliament, and the Commissioner for Human Rights of the Council of Europe. Aidan has been called to the Bar of England and Wales.

Intelligence services perform a valuable service to democratic societies in protecting national security, including safeguarding the fundamental freedoms and human rights of their members. The secret nature of intelligence work can, however, put the services at odds with the principles of an open society. This applies in particular to international cooperation, where intelligence services try to keep secret why, how, with whom and when they cooperate with other states. Until relatively recently, international intelligence cooperation was a black box, impenetrable to public scrutiny, about which states gave very little or no information. The secrecy surrounding international cooperation was so high that it was thought to be impossible to address issues of accountability.

Against this backdrop, the aim of the guide is to provide practical and specific guidance on how accountability and oversight of international intelligence cooperation can be strengthened on the basis of practical examples. It is based on international comparative research of legal and institutional frameworks of intelligence oversight, combined with in-depth interviews with former intelligence officials and intelligence overseers. It covers recent developments in intelligence cooperation, domestic and international standards, as well as internal and external oversight of international cooperation. The guide is an invaluable and practical tool for everyone concerned about accountability in this important but challenging field.

The guide is the result of a multi-year cooperation research project of the Geneva Centre for the Democratic Control of Armed Forces (DCAF) and the Norwegian Parliamentary Intelligence Oversight Committee.

ISBN 978-92-9222-375-5
Printing Office of the Parliament of Norway.