HOMELAND SECURITY PROGRAM and the INTELLIGENCE POLICY CENTER

THE ARTS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND HOMELAND SECURITY
TRANSPORTATION AND INFRASTRUCTURE
WORKFORCE AND WORKPLACE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

Jump down to document

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

Purchase this document

Browse Books & Publications

Make a charitable contribution

For More Information

Visit RAND at www.rand.org

Explore the RAND Homeland Security Program

RAND Intelligence Policy Center

View document details

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Unauthorized posting of RAND PDFs to a non-RAND Web site is prohibited. RAND PDFs are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see RAND Permissions.

This product is part of the RAND Corporation monograph series. RAND monographs present major research findings that address the challenges facing the public and private sectors. All RAND monographs undergo rigorous peer review to ensure high standards for research quality and objectivity.

Considering the Creation of a Domestic Intelligence Agency in the United States

Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom

BRIAN A. JACKSON, EDITOR

Contributors: Peter Chalk, Richard Warnes, Lindsay Clutterbuck, Aidan Kirby

Prepared for the Department of Homeland Security

RAND HOMELAND SECURITY PROGRAM and the INTELLIGENCE POLICY CENTER

This research was sponsored by the United States Department of Homeland Security and was conducted jointly under the auspices of the Homeland Security Program within RAND Infrastructure, Safety, and Environment and the Intelligence Policy Center of the National Security Research Division.

Library of Congress Cataloging-in-Publication Data

Considering the creation of a domestic intelligence agency in the United States : lessons from the experiences of Australia, Canada, France, Germany, and the United Kingdom / Brian A. Jackson, editor.
p. cm.
Includes bibliographical references.
ISBN 978-0-8330-4617-8 (pbk. : alk. paper)
1. Intelligence service—United States. 2. Intelligence service—Western countries. 3. Terrorism—United States—Prevention. 4. Terrorism—Government policy—United States. I. Jackson, Brian A.

JK468.I6C66 2009
363.28—dc22

2008046790

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

Cover photo courtesy of AP Photo/Mary Altaffer.

© Copyright 2009 RAND Corporation

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from RAND.

Published 2009 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Preface

With terrorism still prominent on the U.S. national agenda, whether the country's prevention efforts match the threat it faces continues to be central in policy debate. One element of this debate is questioning whether the United States, like some other countries, needs a dedicated domestic intelligence agency. To examine this question, Congress directed that the U.S. Department of Homeland Security Office of Intelligence and Analysis perform "an independent study on the feasibility of creating a counter terrorism intelligence agency" (U.S. Congress, 2006, p. 122). The results of this study are presented in three volumes:

- This volume contains case studies of other nations' domestic intelligence organizations and activities.
- An additional volume, published separately, *The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency* (Jackson, 2009), presents a series of papers examining the U.S. context for domestic intelligence, current activities, and varied approaches for assessing options.
- The overarching policy results of the assessment, including a discussion of the pros and cons of creating a new intelligence organization, are included in a companion volume to this work: *Reorganizing U.S. Domestic Intelligence: Assessing the Options* (Treverton, 2008).

This volume should be of interest to homeland security policymakers, state and local governments, law enforcement organizations, civil rights and civil liberties organizations, and private-sector organizations with interests in homeland security. This study is part of a larger body of RAND research related to homeland security, intelligence, and terrorism. Related RAND publications include the following:

- Peter Chalk and William Rosenau, *Confronting the "Enemy Within": Security Intelligence, the Police, and Counterterrorism in Four Democracies*, MG-100-RC, 2004
- K. Jack Riley, Gregory F. Treverton, Jeremy M. Wilson, and Lois M. Davis, *State and Local Intelligence in the War on Terrorism*, MG-394-RC, 2005
- Brian A. Jackson, Peter Chalk, Kim Cragin, Bruce Newsome, John V. Parachini, William Rosenau, Erin M. Simpson, Melanie Sisson, and Donald Temple, *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*, MG-481-DHS, 2007.

The RAND Homeland Security Program

This research was conducted jointly under the auspices of the Homeland Security Program within RAND Infrastructure, Safety, and Environment and the Intelligence Policy Center of the National Security Research Division. The mission of RAND Infrastructure, Safety, and Environment is to improve the development, operation, use, and protection of society's essential physical assets and natural resources and to enhance the related social assets of safety and security of individuals in transit and in their workplaces and communities. Homeland Security Program research supports the Department of Homeland Security and other agencies charged with preventing and mitigating the effects of terrorist activity within U.S. borders. Projects address critical infrastructure protection, emergency management, terrorism risk man-

agement, border control, first responders and preparedness, domestic threat assessments, domestic intelligence, and workforce and training.

Information about the Homeland Security Program is available online (http://www.rand.org/ise/security/). Inquiries about homeland security research projects should be addressed to

Andrew Morral, Director
Homeland Security Program, ISE
RAND Corporation
1200 South Hayes Street
Arlington, VA 22202-5050
703-413-1100, x5119
Andrew_Morral@rand.org

The RAND Intelligence Policy Center

The Intelligence Policy Center is part of the RAND National Security Research Division (NSRD). NSRD conducts research and analysis for the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the defense agencies, the Department of the Navy, the Marine Corps, the U.S. Coast Guard, the U.S. Intelligence Community, allied foreign governments, and foundations.

For more information on RAND's Intelligence Policy Center, address queries to

John Parachini, Director
Intelligence Policy Center
RAND Corporation
1200 South Hayes Street
Arlington, VA 22202-5050
703-413-1100, x5579
John_Parachini@rand.org

More information about RAND is available at www.rand.org

Contents

Figure and Tables

Figure

Tables

Acknowledgments

Like many RAND projects, this study relied on the efforts and contributions of a number of individuals inside RAND beyond those who are listed as authors of the chapters, as well as a variety of people outside of RAND who made critical contributions to the study.

First, we would like to acknowledge the contribution of our colleague and co–project leader for the study, Gregory Treverton. Greg's involvement significantly shaped the conduct of the project, and his experience and views were instrumental in shaping elements of the analyses included in this volume. In addition to the individual authors listed on the chapters, other RAND staff made important contributions to the conduct of the project, including, in alphabetical order, Mike Hix, Gordon T. Lee, Andrew R. Morral, John Parachini, K. Jack Riley, Lynn M. Scott, Douglas Shontz, Jerry M. Sollinger, and Katharine Watkins Webb. As part of the review of the various project documents and reports by experts both inside and outside RAND, Daniel Byman, James B. Bruce, Charles Nemfakos, Paul C. Light, and Paul R. Pillar all made important contributions to our thinking.

During our research, we reached out to experts and practitioners in the relevant fields and spoke to a wide range of individuals, only some of whom we can identify by name. A number of individuals inside and outside government at the federal, state, and local levels gave generously of their time and expertise in interviews with various project team members. However, because interviews were conducted on a not-for-attribution basis, we do not name those contributors in this monograph. The project also benefited from the involvement of a panel

of eminent experts in intelligence, law enforcement, and related areas who provided input at a key point in the study. The members of that expert panel, also listed alphabetically, were Marion Bowman, John Brennan, Joan Dempsey, Michael German, Richard Jerome, Richard Posner, Suzanne Spaulding, John P. Sullivan, and John Yoo.

We would also like to acknowledge the contribution of Erin-Elizabeth Johnson of RAND Publications and Creative Services, whose careful and comprehensive edit of the document greatly improved the final product.

Abbreviations

AAT	Administrative Appeals Tribunal
AD	Action Directe [Direct Action]
AFP	Australian Federal Police
AG	Attorney-General
AIC	Australian intelligence community
ANAO	Australian National Audit Office
AQMI	Al-Qaida pour le Maghreb Islamique [al Qaeda for the Islamic Maghreb]
ASALA	Armenian Secret Army for the Liberation of Armenia
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
AUSTRAC	Australian Transaction Reports and Analysis Centre
BCRA	Bureau Central de Renseignements et d'Action [Central Office of Intelligence and Operations]
BfV	Bundesamtes für Verfassungsschutz [Federal Office for the Protection of the Constitution]
BGS	Bundesgrenzschutz [federal border guards]

BKA	Bundeskriminalamt [federal criminal police]
BLU	Business Liaison Unit
BMI	Bundesministerium des Innern [Federal Ministry of the Interior of the Federal Republic of Germany]
BND	Bundesnachrichtendienst [Federal Intelligence Service]
BSI	Bundesamtes für Sicherheit in der Informationstechnik [Federal Office for the Security of Information Technology]
BVerfSchG	Bundesverfassungsschutzgesetz [Federal Law for the Protection of the Constitution]
C-36	the Anti-Terrorism Act of Canada
CBRNE	chemical, biological, radiological, nuclear, or explosive
CBSA	Canada Border Services Agency
CHIS	covert HUMINT source
CI	critical infrastructure
CIA	Central Intelligence Agency
CIC	Canadian intelligence community
CID	Criminal Investigation Department
CILAT	Comité Interministériel de Lutte Anti-terroriste [Interministerial Committee for the Anti-Terrorist Struggle]
CNI	Critical National Infrastructure
CPNI	Centre for the Protection of National Infrastructure
CSIS	Canadian Security Intelligence Service

CT	counterterrorism
CTIU	Counter Terrorism Intelligence Unit
CTU	Counter Terrorism Unit
DCRG	Direction Centrale des Renseignements Généraux [Central Directorate of General Intelligence]
DCRI	Direction Centrale du Renseignement Intérieur [Central Directorate of Interior Intelligence]
DG	Director-General
DGSE	Direction Générale de la Sécurité Extérieure [General Directorate for External Security]
DIGO	Defense Imagery and Geospatial Organisation
DNAT	Division Nationale Anti-terroriste [National Anti-Terrorist Division]
DND	Department of National Defence
DRM	Direction du Renseignement Militaire [Military Intelligence Directorate]
DSD	Defense Signals Directorate
DST	Direction de la Surveillance du Territoire [Directorate of Territorial Surveillance]
FBI	Federal Bureau of Investigation
FLN	Front de Libération Nationale [National Liberation Front]
FRG	Federal Republic of Germany
GCHQ	Government Communications Headquarters
GDR	German Democratic Republic
GIA	Groupe Islamique Armé [Armed Islamic Group]

GIGN	Groupe d'Intervention de la Gendarmerie Nationale [Intervention Group of the National Gendarmerie]
GSG 9	Grenzschutzgruppe 9 [Border Guard Group 9]
GSPC	Groupe Salafiste pour la Prédication et le Combat [Salafist Group for Prayer and Combat]
GTAZ	Gemeinsamen Terrorismusabwehrzentrum [Joint Counterterrorism Center]
HMRC	Her Majesty's Revenue and Customs
HUMINT	human intelligence
HVA	Hauptverwaltung Aufklärung [East German administration]
IGIS	Inspector-General of Intelligence and Security
IGPN	inspection Générale de la Police Nationale [General Inspectorate of the National Police]
IJU	Islamic Jihad Union
INTERPOL	International Criminal Police Organization
IPT	Investigatory Powers Tribunal
IRA	Irish Republican Army
ISC	Intelligence and Security Committee
ITAC	Integrated Threat Assessment Centre
JCTICU	Joint Counter-Terrorism Intelligence Coordination Unit
JI	Jemaah Islamiya
JTAC	Joint Terrorism Analysis Centre
KGB	Komityet Gosudarstvennoy Bezopasnosty [Committee for State Security]

LfV	Landesamt für Verfassungsschutz [regional intelligence organization]
LKA	Landeskriminalamt [regional or state criminal police]
LTTE	Liberation Tigers of Tamil Eelam
MAD	Militärische Abschirmdienst [Military Intelligence Service]
MfS	Ministerium für Staatssicherheit [Ministry for State Security]
MI5	U.K. Security Service
NADIS	Nachrichtendienstliche Informationssystem [Intelligence Service Information System]
NAO	National Audit Office
NCTC	National Counter-Terrorism Committee
NPD	Nationaldemokratische Partei Deutschlands [German National Democratic Party]
NSA	National Security Agency
NTAC	National Threat Assessment Centre
OAS	Organisation de l'Armée Secrète [Organization of the Secret Army]
ONA	Office of National Assessments
OSCT	Office for Security and Counter-Terrorism
PCF	Parti Communiste Français [French Communist Party]
PDS	Partei des Demokratischen Sozialismus [Democratic Socialist Party]

PJCIS	Parliamentary Joint Committee on Intelligence and Security
PKGr	Parlamentarische Kontrollgremium [Parliamentary Standing Committee for the Intelligence Services]
PKK	Partiya Karkerên Kurdistan [Kurdish Workers' Party]
PM&C	Department of the Prime Minister and Cabinet
PMV	politically motivated violence
PSEP	Minister of Public Safety and Emergency Preparedness
RAF	Rote Armee Fraktion [Red Army Faction]
RCMP	Royal Canadian Mounted Police
RER	Réseau Express Régional [Regional Express Network]
RIPA	Regulation of Investigatory Powers Act 2000
SA	Service Action [Action Service]
SCoNS	Secretaries Committee on National Security
SDAT	Sous-Direction Anti-terroriste [Anti-Terrorist Sub-Directorate]
SGDN	Secrétariat Général de la Défense Nationale [General Secretariat of National Defense]
SIGINT	signals intelligence
SIM	subscriber identity module
SIRC	Security Intelligence Review Committee
SIS	Secret Intelligence Service
SOCA	Serious Organised Crime Agency

SWAG	Special Weapons Analysis Group
TA	threat assessment
TARC	Target and Approval and Review Committee
TEL	terrorist-entity listing
TRA	threat and risk assessment
UCLAT	Unite de Coordination de la Lutte Anti-terroriste [Coordination Unit for the Anti-Terrorist Struggle]

CHAPTER ONE

Introduction

In the current environment, the threat of terrorism is a major shaping force of many nations' international and domestic security policies. Nonstate groups with the intent and capability to take violent action are a reality in many countries given the existence of international movements, such as al Qaeda, that have the capacity to direct or inspire violence across the world, thereby creating another source of threat and risk. The threat of terrorist activity extends across a wide spectrum, from attacks causing little in the way of injury or damage to the potential for large-scale incidents. Although the probability of such high-consequence scenarios occurring is comparatively low, their ability to cause national-scale outcomes has meant that governments have focused their efforts on seeking to prevent them.

The core of government attempts to prevent violent and other criminal activity is intelligence and law enforcement, which, for many years, were viewed by Americans as separate activities. Put in place mainly to address the threat posed by agencies and agents of foreign governments, intelligence was viewed as an internationally focused activity that occurred largely outside U.S. borders. Intelligence agencies were charged with gathering information and learning about threats to the country, not prosecuting the perpetrators; these activities were designed to make it possible to take action to prevent attacks from happening. Law enforcement, in contrast, was done "at home" and, while certainly designed to help deter or prevent criminal activity, was largely a reactive enterprise. Law enforcement organizations, which generally did not act until after something had already happened, aimed to make

it possible to identify, apprehend, and punish those who broke the law. Differences between what Americans were comfortable with happening outside U.S. borders and which activities targeting Americans they thought should be prohibited to safeguard freedom from government intrusion meant that these two sets of activities were conducted under very different sets of rules, and barriers of various kinds—colloquially referred to as a "wall" to illustrate their perceived effect—were built between them.

For many Americans, the attacks of September 11, 2001, called into question the fundamental assumptions that had underpinned U.S. intelligence and law enforcement activities. Actions by foreign individuals that were carried out largely within the United States resulted in a single attack that killed thousands of people. The boundary between intelligence agencies that had information and law enforcement organizations that could act domestically was viewed as part of the reason the attack was successful.

Perceived changes in the threat posed to the United States led to demand for more, and more effective, terrorism prevention and preparedness activities. According to some, these demands required a change in the way intelligence and law enforcement activities are carried out domestically and a significant alteration in the ground rules that regulate government monitoring and intervention activities within the United States. According to this view, to prevent future attacks, "intelligence must come home" and the government must be able to use data on persons and organizations located in the United States. At the same time, the United States has a history of distrusting centralized government power and, as a result, has often restrained government control over the lives and activities of individual citizens. The fact that responses to threats have consequences of their own—including the potential to significantly change the nature and character of the country—emphasizes the need to assess how intelligence activities can be sufficiently responsive while remaining acceptable to the population they are designed to protect.

Defining Domestic Intelligence

What do we mean by the term *domestic intelligence*? The term *intelligence* sparks a range of associations, many of which stem from intelligence's connection with the secret activities of governments seeking to advance their interests in international affairs. In recent years, the term *intelligence* has been integrated into domestic law enforcement and public safety agencies as part of the phrase *intelligence-led policing*. Definitions of *intelligence-led policing* vary, but common elements include the use of information-gathering capabilities and the analysis and application of resulting information in crime prevention and response activities in addition to their more traditional use in the prosecution of past criminal acts (see, e.g., Weisburd and Braga, 2006; Milligan, Clemente, and Schader, 2006; Ratcliffe, 2002; Peterson, 2005). Use of the term *intelligence* has also spread beyond government organizations into private-sector organizations and elsewhere.[1] To some, the term is most closely associated with the collection of information; others see intelligence as a more general category that includes a much broader range of activities. Such variety in the use and understanding of these terms complicates policy debate, and the lack of standard definitions for intelligence activities focused on homeland security and domestic counterterrorism (CT) efforts has been cited as a significant impediment to designing and assessing policy in this area (Masse, 2003, 2006).

To guide the work reported in this volume, we define *domestic intelligence* as efforts by government organizations to gather, assess, and act on information about individuals or organizations in the United

[1] For example, an entire body of literature has grown around the concepts of business intelligence and competitive intelligence. The literature examines how data and information are collected, analyzed, and applied by the private sector to build or defend competitive advantage in the market.

States or U.S. persons elsewhere[2] that are *not related to the investigation of a known past criminal act or specific planned criminal activity*.[3]

It is often the case that an individual or organization that carries out a terrorist attack—or has specific plans to do so (e.g., the attacker has conspired to acquire weapons for a future attack)—has committed one or more specific crimes. In these cases, traditional law enforcement approaches for investigating and prosecuting these crimes apply. The major difference between intelligence approaches and those used during traditional law enforcement stems from the former's emphasis on preventing future events—i.e., on acting when the individuals or organizations planning an attack may not yet have committed any prosecutable criminal offenses. Intelligence activities can be *investigative* in nature and may resemble law enforcement activities. However, they do not have to satisfy the same legal requirements that constrain the initiation of a law enforcement investigation. An example of such an intelligence activity is investigating a tip about the suspected terrorist behavior of an unknown group to determine whether the tip is credible and, if it is, acting to prevent the attack. However, given substantial concern about the ability of even a single individual working alone to plan and execute acts of terrorist violence, investigative follow-up may not be enough to address the threat of terrorism. As a result, another type of intelligence effort can be more *explorative* in character,

---

[2] Federal law and executive order define a U.S. person as "a citizen of the United States, an alien lawfully admitted for permanent residence, an unincorporated association with a substantial number of members who are citizens of the U.S. or are aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the U.S." (NSA, undated). Although this definition would therefore allow information to be gathered on U.S. persons located abroad, our objective was to examine the creation of a domestic intelligence organization that would focus on—and whose activities would center around—individuals and organizations located *inside the United States*. Though such an agency might receive information about U.S. persons that was collected abroad by other intelligence agencies, it would not collect that information itself.

[3] As our discussion of intelligence-led policing suggests, traditional law enforcement does indeed involve the collection and use of information that is not linked to specific criminal activities. However, activities we consider *domestic intelligence* differ in the scope and breadth of effort involved. Domestic intelligence activities are not a new phenomenon; see, for example, discussion in Morgan, 1980, p. 13.

seeking proactively to (1) identify individuals or groups that might be planning violent actions and (2) gather information that might indicate changes in the nature of the threat to the country more broadly (see, e.g., DeRosa, 2004). Such explorative activity inherently involves gathering a broader spectrum of data about a greater number of individuals and organizations who are unlikely to pose any threat of terrorist activity.

Our definition of *domestic intelligence* parallels those that appear in the academic literature that has examined U.S. policy in this area over the past several decades (see, e.g., Morgan, 1980). However, it is narrower than more-general definitions that seek to capture the full breadth of intelligence requirements associated with homeland security or homeland defense.[4] Our focus on the collection and use of information about individuals and organizations means that we have focused on the tactical threat-identification and threat-disruption parts of homeland security intelligence. Thus, we do not consider activities such as analyses designed to identify societal vulnerabilities or map the threat to those identified vulnerabilities to guide broader homeland security policies.[5] Others have noted that the boundary between intelligence and law enforcement activities has blurred over time, particularly in response to transnational threats such as drug trafficking and terrorism. This blurring of the boundary between the two complicates an examination focused largely on the CT mission.[6]

---

[4] For a more general review of homeland security intelligence, see Masse, 2006.

[5] The 2002 *National Strategy for Homeland Security* (Office of Homeland Security, 2002, pp. 15–19) includes a four-part breakdown of homeland security intelligence and information-analysis roles and responsibilities: (1) tactical threat analysis, (2) strategic analysis of the enemy, (3) vulnerability assessment, and (4) threat-vulnerability integration, or "mapping." Though this taxonomy was not included in the 2007 version of the national strategy, we found it useful for defining the scope of the domestic intelligence activities considered during this study. Similar broad definitions are suggested in Markle Foundation Task Force, 2002, and Gilmore Commission, 2002, p. iv.

[6] See, for example, discussion in Best, 2001. This blurring—and the difficulty of crafting clear boundaries between activities focused on national security threats and those focused on aiding "in the capture of prospective or practicing criminals"—was cited as a particular difficulty in a review of Department of Homeland Security intelligence activities in June 2007 (DHS OIG, 2007, p. 3).

Arguments for Change in Current Domestic Intelligence Policies

Because of the prominence of the terrorist threat, particularly in the years since the 9/11 attacks, how the United States has responded to the threat of terrorism, the effectiveness of the steps that have been taken, and the appropriateness of such steps given deeply held values of personal freedom and liberty have been prominent questions in public and policy discussions. Nationally chartered commissions, nongovernmental organizations, scholars, commentators across the political spectrum, and the public have weighed in on various issues related to CT and intelligence. Most of these discussions have addressed terrorism and intelligence writ large, covering issues relevant to *all* national intelligence efforts, domestic and foreign, rather than domestic intelligence alone. Others have been specific to domestic intelligence activities. The following issues that are relevant and central to the consideration of a new domestic intelligence agency have been raised:[7]

1. **The difficulty of identifying a small number of threatening individuals in the general population of a large and diverse nation.** Terrorism will always be a threat posed to the many by the few, which means that intelligence activities must detect weak signals of threat behaviors against a strong background of legitimate activity. There are concerns that U.S. domestic intelligence efforts, as currently constituted, may not be sufficient to detect all threats to the country.
2. **The need for sufficient adaptability to respond to dynamic threats.** Many terrorist organizations have demonstrated that they can rapidly alter their behavior and adapt their tactics in the face of CT pressure. To keep pace with an agile threat, intelligence organizations must be able to adapt as well. Large, bureaucratic organizations frequently face challenges in doing

[7] Of these issues, the first two—the difficulty of identifying a small number of threatening individuals against a large background of other people and the need for adaptability—are problems relevant to all intelligence efforts. The remaining issues are specific to domestic intelligence activities.

so, and the ability to change rapidly may conflict with other objectives—including societal goals of intelligence oversight.

3. **Problems in interagency cooperation.** In contrast to foreign intelligence, which mainly involves federal organizations, domestic intelligence is an inherently interagency and multilevel enterprise. The United States has thousands of independent law enforcement organizations, and government and nongovernmental entities not normally associated with security missions (e.g., the fire service and private-sector firms) may have information that could indicate threatening activity. The involvement of many organizations in intelligence activities has always posed a risk of breakdowns in information sharing, turf battles, and bureaucratic duplication and inefficiency.
4. **Differences in the ways in which law enforcement and intelligence organizations operate.** Preventing terrorism domestically inherently straddles functions that have historically been divided between law enforcement and intelligence agencies. In the United States, law enforcement organizations—most notably, the Federal Bureau of Investigation (FBI)—have central roles in domestic intelligence activities related to the prevention of terrorism. These different types of organizations have distinct cultures and have generally focused their efforts quite differently, leading to questions about whether the two can be mixed effectively and whether doing so undermines the nation's ability to detect and prevent terrorism. Separating intelligence efforts from law enforcement activities has been an argument for changing domestic intelligence organizations and activities.
5. **Concern about the effect of intelligence activities on personal privacy and civil liberties.** Intelligence activities that require government intrusion into individuals' private lives raise significant and real concerns about the effect of those activities on individuals and on the character of the nation, entities that such activities are intended to protect. Since 9/11, some people have raised questions about the type of information the U.S. government has gathered on individuals and organizations in the United States and about how that information has been col-

> lected and used. Throughout the history of U.S. domestic intelligence, questions about how long the government should store intelligence data about individuals—and about how responsive the government is to direction to destroy those data—have come up repeatedly.

All of these factors have been cited as rationales for changing the way in which domestic intelligence and CT activities are carried out.

About This Study

In spite of significant changes to U.S. domestic intelligence activities in recent years, questions remain about whether the United States has the right organizational and technical tools in place to protect the nation. One element of this debate is the question of whether the United States needs a dedicated domestic intelligence agency. The argument that such an agency is necessary has been raised during policy debates and considered by a number of national commissions that address U.S. domestic security and the threat of terrorism. Such a policy change is, of course, only one of many possible changes that could be made in U.S. CT policy, but it is one that recurs in policy discussions[8] and could be a reaction to a future terrorist attack on the United States.

To examine this potential policy change, Congress directed that the U.S. Department of Homeland Security Office of Intelligence and Analysis perform "an independent study on the feasibility of creating a counter terrorism intelligence agency" (U.S. Congress, 2006, p. 122). If such an agency were built, the major rationale for doing so would be the desire to improve security and the belief that a new agency would be more *capable* of protecting the country from terrorism than are current domestic intelligence efforts. However, given significant concerns about the effect of security and intelligence policies on the American people, privacy, and the character of the country, any new organization

[8] For example, discussion during October 2007 congressional hearings as reported in Johnson, 2007.

would also have to be *acceptable* to the public. RAND was not asked to make a definitive recommendation about whether to create such an agency but was charged with examining relevant options and issues in order to frame policy choices.

In considering the potential creation of a new domestic intelligence agency, we approached the issue from a variety of directions, seeking insights that would help us understand the pros and cons of creating such an organization and describe different approaches for doing so. This research effort resulted in a set of topical papers and analyses that address different parts of this policy issue and examine it from different perspectives. The overall study examined both issues associated with and approaches to understanding the U.S. domestic context for domestic intelligence and ways of examining the decision to create a new domestic intelligence agency. In addition, we examined the histories of several nations that already have such an agency in an effort to learn from their experiences. This volume presents our case studies of other nations' domestic intelligence organizations.

Examining Other Nations' Experiences with Domestic Intelligence

The United States does not have a stand-alone domestic intelligence agency, but a variety of other countries do. The UK Security Service (better known as MI5) is a frequently cited example, though an array of other democracies have similar agencies. The experiences of those nations in creating, managing, and assessing the results of their domestic intelligence efforts are a source of information relevant to the decision to create such an organization in the United States.

As part of this research effort, we examined the domestic intelligence organizations of five nations that have stand-alone domestic intelligence agencies. In selecting countries, we chose the following democracies whose values and practices make their experiences most relevant to the U.S. context: Australia, Canada, France, Germany, and the United Kingdom. Based on both the published literature and our interviews with relevant experts and practitioners in each country, we produced a case study of each country's experience. Each case study

was guided by a common template of focus areas, described below, allowing us to create five parallel studies:[9]

1. **Creation and relevant history:** Has the domestic intelligence service's basic nature changed since its creation? What was the organizational context when the service was created?
2. **Mission and critical capabilities:** Is the service focused on terrorism or another specific mission? How large is its staff, and what are its key capabilities? With what methods does it accomplish its mission?
3. **Leadership and human capital:** What source provides the service with its leaders? Have these leaders been career professionals, leaders in related sectors or institutions, or outsiders? How has the organization met its human-capital needs for qualified individuals below the leadership level and for all intelligence functions?
4. **Management and process:** To whom or to what body does the service report on a day-to-day basis? How does it make decisions about, for instance, initiating surveillance and other activities, and how are those activities approved? Does this service have procedures for gaining feedback on activities, and does this feedback result in process changes?
5. **Organizational structure and funding patterns:** How has the service been designed to fulfill its mission and critical capabilities? How is it funded, and how are resource-allocation decisions made?
6. **Key relationships with other intelligence and law enforcement agencies:** Are these relationships defined in statutes or formal procedures, or have they simply developed over time?
7. **Oversight:** Apart from management procedures, are there executive, legislative, or other oversight bodies or mechanisms? How do they work? To the extent that this can be judged, how effec-

[9] The factors that framed the case studies (including the nine factors listed here and a tenth that focuses on each case's relevant lessons for the United States) were crafted primarily by our colleague and co–project leader, Gregory Treverton. His contribution to defining the structure of and providing the frame for the case studies is gratefully acknowledged.

tive are they at discovering and calling to attention mistakes or abuses?

8. **Performance metrics:** How do the service and the nation judge the effectiveness of the organization's work? Are there formal metrics or processes? What measures dominate government and public discussion of the service and its work?
9. **Problems or controversies:** Have episodes (or allegations) of crisis, corruption, or abuse been part of the service's or the country's history? How have they affected the service's work?

These focus areas provided a common structure for the chapters on each country. We also looked across the experiences of the various nations to identify relevant lessons that could inform the decision to create such an agency in the United States.

About This Volume and Companion Volumes from the Study

Chapters Two through Six of this volume present our case studies of domestic intelligence efforts in five democratic states. Chapter Seven looks across the case studies to examine the changes that have occurred in these countries since 2001 and the performance of the intelligence services. Chapter Eight presents our conclusions and a discussion of lessons for the United States.

This volume is one of three RAND publications that resulted from this research effort. The other publications are a cross-cutting policy document examining the pros and cons of creating a new intelligence organization (Treverton, 2008) and a companion volume containing the remainder of the research papers that resulted from our study of the U.S. context for domestic intelligence (Jackson, 2009).

CHAPTER TWO

Australia

Peter Chalk

Australia has been largely free of domestic and imported terrorism in the past and still does not face the level of threat experienced by states in North America and Western Europe.[1] However, there is little question that the country's overall risk profile has been substantially heightened as a result of former Prime Minister John Howard's close alliance with the United States and his government's decision to host, lead, or support the following prominent international events: the 2000 Olympic Games in Sydney; the 2002 Commonwealth Heads of Government Meeting in Brisbane; the 1999–2000 International Force for East Timor intervention,[2] which generated enormous opposition throughout Indonesia and the wider Muslim world, not least because it was instrumental in creating an independent Catholic state out of the world's largest Islamic polity; and the post-9/11 war against al Qaeda.[3] At the same time, globalization and increased volumes of cross-border movements of people, money, and commodities have rendered redundant the traditional defense afforded to the country by its geography.[4]

---

[1] To date, the most significant act of Australian domestic terrorism in Australia (that is, an act carried out in Australia by an Australian national) was the 1978 bombing of the Sydney Hilton Hotel, which left three people dead and eight injured.

[2] For an overview of Australia's role in this intervention, see Chalk, 2001.

[3] Along with the UK, Australia has been the most forceful proponent of the United States' post–9/11 war against terrorism.

[4] Author telephone interviews, June 2007 and October 2007 (see also PM&C, 2006, pp. 7–9, and Grono, 2004).

Currently, the main threat to Australia's internal and regional security emanates from Islamist extremists connected with either al Qaeda or the Indonesia-based Jemaah Islamiya (JI) network. The latter group has already been implicated in several attacks that have directly affected the country, including, notably, the October 2002 and October 2005 suicide strikes in Bali (which, combined, killed 92 Australians)[5] and the 2004 bombing of Canberra's embassy in Jakarta.[6] Moreover, there is widespread speculation that certain homegrown militant cells have made contact with al Qaeda, allegedly to undertake attacks, on their own initiative, in furtherance of bin Laden's self-defined jihadist objectives. Concerns in this regard were dramatically highlighted by the November 2005 arrests of 18 suspected Islamist terrorists who were alleged to have been plotting a series of attacks against several high-profile venues across the country, including the civilian nuclear-power reactor at Lucas Heights, just outside Sydney (see, e.g., Callinan, 2005; "Sydney Nuclear Power Plant Was a Possible Target," 2005; "Terror Swoop," 2005; "Australia Nabs 16 in Terror Raids," 2005; King, 2006).

At the time of this writing, the overall threat of so-called foreign-inspired political violence was deemed to be significant, enduring, and evolving. Countering this challenge has, accordingly, continued to occupy the bulk of the operational and analytical resources allocated to the country's principal domestic intelligence agency, the Australian Security Intelligence Organisation (ASIO).

Creation and Relevant History

ASIO was created in 1949 following revelations that the Soviet Union was running a spy ring in the Australian government. Emerging from the remnants of the Commonwealth Investigation Service,[7] it was con-

---

[5] The first Bali attack killed 88 Australians; the second killed four.

[6] For further details on JI, see Ministry of Home Affairs, 2003; ICG, 2003, 2007; Rabasa et al., 2006, Chapter 11; Chalk, 2005.

[7] The Commonwealth Investigation Service was the successor to the Allied Intelligence Bureau, which was created in 1942 as a conglomeration of U.S., Australian, British, and

verted to a statutory body in 1956 and derives its current authority from the Australian Security Intelligence Organisation Act of 1979.[8] The agency has no independent powers of arrest—although since 2003, it has had the limited right, if it works through the Australian Federal Police (AFP), to detain suspected terrorists for questioning—and is concerned solely with collecting and analyzing information on threats to the country's internal security (Chalk and Rosenau, 2004, p. 35; ASIO, 2006, p. viii, 42; Burch, 2007, p. 9).

For much of its early history, ASIO focused the bulk of its attention on counterintelligence. During the 1960s, 1970s, 1980s, and 1990s, these counterintelligence activities were directed toward monitoring known or suspected communist agents, sympathizers, and agitators; frustrating their efforts to gain scientific, technical, military, and political information; and ensuring that Australian citizens would not be co-opted or pressured into furthering the interests of another country at the expense of Australia's interests.[9]

The end of the Cold War, the rise of al Qaeda, preparations for the 2000 Olympic Games in Sydney, the 9/11 attacks, and the emergence of extremist jihadist networks that link militants in Southeast and Southwest Asia and the Middle East combined to significantly alter the thrust of ASIO's operational agenda, which is now aimed squarely at countering Islamist extremism.[10] Significantly, the focus on this threat has caused the agency to systematically revisit the wisdom of bounding its operational agenda in strictly geographic terms.[11] As one official remarked,

---

Dutch security agencies tasked with garnering information on the activities of Imperial Japan in the Asia-Pacific.

[8] This legislation specifically designates ASIO as Australia's principal national agency responsible for countering espionage, terrorism, and politically motivated violence (PMV).

[9] Author interviews, Canberra, October 2007. For a good account of the agency's activities during this period, see McKnight, 1994.

[10] Author telephone interview, June 2007; Burch, 2007, p. 9. This thrust was explicitly spelled out in the agency's 2006 *Report to Parliament*, which stressed that its primary focus is "the prevention of harm to Australians and Australian interests from threats to security, particularly the threat of terrorism from Islamic extremists" (ASIO, 2006, p. 3).

[11] Author interviews, Canberra 2007.

> [In today's world,] the notion of domestic CT intelligence has become a misnomer. Most of the current dangers to Australia originate from outside the country's sovereign borders. Restricting the activities of ASIO to internal information gathering is thus inappropriate and unlikely to meet the specific challenges posed by the contemporary terrorist phenomenon.[12]

Although mitigating jihadist-inspired terrorism remains ASIO's main focus, the agency continues to play an active role in addressing other challenges to national security. This role is supported by the general mission statement set forth in the ASIO Act of 1979 and currently includes preventing foreign interference in the Australian government's processes and internal affairs, containing local manifestations of racist and ethnonationalist fanaticism, preempting violent civil disturbances and protests, and counterproliferation. These latter activities, however, account for only 20 percent (approximately) of ASIO's time and workload.[13]

Mission and Critical Capabilities

ASIO defines its mission in the following terms: "to identify and investigate threats to security and provide advice to protect Australia, its people and its interests" (ASIO, 2007b, p. iii). As previously noted, domestic CT constitutes ASIO's main area of responsibility, occupying most of the agency's resources.

First and most fundamentally, ASIO issues regular threat assessments, which are based on raw data that are evaluated by dedicated analysts who are career-track staff but are not necessarily subject-matter experts.[14] These threat assessments are either tactical or strategic. The former are time-sensitive assessments that focus on the likelihood and probable nature of threats to the security of specific people, places,

---

[12] Author telephone interview, June 2007.

[13] Author telephone interview, June 2007; ASIO, 2006, pp. 22–25.

[14] ASIO personnel are rotated between intelligence desks at least every three years, and often more frequently.

and events; they are generated on ASIO's own initiative or in response to requests from federal government departments, state and territory officials, and the police. Longer-term strategic assessments are concerned almost exclusively with the evolving dynamics of international and regional terrorism and they currently give priority to developments taking place in al Qaeda, JI, and the Iraqi insurgency. Although ASIO does not produce an annual threat assessment on terrorism per se, comprehensive reports on PMV are produced on a regular basis, providing context for the statutory annual parliamentary audit of the agency's activities.[15]

In addition to threat identification, ASIO fulfills important security-advisory functions, both for critical infrastructure (CI) protection and personnel vetting. The agency's Business Liaison Unit (BLU) acts as a central interface with the owners and operators of Australia's CI,[16] who are by and large either working in the private sector or contracting to state and territory governments on a commercial basis. The BLU runs outreach programs to ensure that relevant members of the business community can access comprehensive information on any matter that could affect the integrity of CI assets or the staff for whom they are responsible. ASIO is also a major participant in the Trusted Information Sharing Network, which allows classified material pertinent to CI protection to be passed to the broader business world,[17] and in the Information Infrastructure Protection Group and the Electronic Secu-

[15] Author interviews, Canberra, November 2003 and January 2006 (see also ASIO, 2006, p. 43). It should be noted that ASIO also contributes to Office of National Assessments (ONA) reports, which are typically produced four times per year.

[16] In Australia, infrastructure assets are categorized as vital, major, significant, or low. At the time of this writing, the following sectors were deemed vital: food, health, energy, utilities, transport, manufacturing, communications, banking and finance, government services and icons, and public gatherings.

[17] The Trusted Information Sharing Network model for disseminating classified information between the federal government and private-sector interests exists in Australia and a few other countries and is generally judged by all participating parties to have worked exceptionally well in terms of helping to connect the dots and provide for holistic threat-remediation strategies on the ground (author interviews, Canberra and Brisbane, January 2006).

rity Coordination Group, both of which help to coordinate policy for safeguarding the country's National Information Infrastructure.[18]

The bulk of ASIO vetting is directed at validating the background and bona fides of those requesting clearance to access classified or sensitive information and at conducting CT checks on trainee pilots, those who regularly work in secured areas of seaports and airports, and those employed in positions that bring them into contact with potentially dangerous explosive material (such as ammonium nitrate). In the case of requests for clearance, ASIO assessments are usually based on material provided by the submitting agency but may also require that ASIO conduct additional interviews or follow-on activities to resolve outstanding issues that arise from initial investigations. In the case of CT checks, ASIO examinations are limited to ascertaining whether the subject has any known links to terrorism and are generally completed within 5–10 days.[19]

ASIO also contributes to Australian border security, constituting the principal source of advice to the Department of Immigration and Multicultural and Indigenous Affairs Movement Alert List. This database contains the names of individuals seeking entry to Australia who are deemed to pose an active or latent national security risk. In addition, ASIO carries out assessments of unauthorized arrivals to whom the Department of Immigration and Multicultural Affairs has granted temporary protection visas to determine whether further extensions of these documents are warranted. Between 2005 and 2006, ASIO processed a total of 3,005 temporary protection visa cases and denied 12 people of various nationalities entry into Australia on the basis of their

---

[18] ASIO, 2006, pp. 27–28. Australia's National Information Infrastructure includes all telecommunications and information networks that support banking and finance, transport, supply chains, energy and utilities, information services, and critical government communications (such as defense and emergency services).

[19] ASIO, 2006, p. 37. Since 2007, ASIO's CT-checking function has been supported by AusCheck, a new body housed in the Department of the Attorney-General (AG) to provide a centralized and nationally consistent approach to ensuring that unsuitable individuals are not able to work in sensitive areas of Australian seaports and airports (see PM&C. 2006, p. 43).

links to PMV, terrorism, or foreign intelligence services (ASIO, 2006, p. 30).

Finally, ASIO runs an active counterproliferation program that is essentially geared toward preventing terrorist groups (and potential state sponsors) from exploiting Australian resources, technical knowledge, and resources to develop chemical, biological, radiological, nuclear, or explosive (CBRNE) weapon potential. As part of this remit, the agency maintains a national database on CBRNE terrorism and, in conjunction with the AFP, the Defense Intelligence Organisation, and the Defense Science and Technology Organisation, runs a dedicated Special Weapons Analysis Group (SWAG) to assess international and regional intelligence on extremist use of unconventional agents for the purpose of mass destruction (ASIO, 2006, pp. 25–26).

In pursuing these various functional tasks, ASIO employs a staff of 1,400 (as of October 2007) and, at the time of this writing, ran on an operational budget of around A$181 million. The agency has been funded to expand to around 1,860 personnel by 2010–2011, the bulk of whom will be dedicated to CT duties.[20]

As might be expected, the bulk of ASIO's work is collecting covert information, which is then used to (1) generate domestic threat assessments that are produced primarily for the police, the wider Australian intelligence community (AIC), government departments, and corporate stakeholders charged with safeguarding components of CI and (2) assist in CT planning and inform associated physical protection and target-hardening programs. Like its counterparts in other Western democracies such as France, Britain, Germany, Italy, and Canada, ASIO derives much of this information from human sources. A certain amount of data emanates from well-placed informants and individuals who submit plea bargains during trials for illegal activity. While this particular form of human intelligence (HUMINT) is often the most valuable to efforts to prioritize targets for covert surveillance or gain preemptive warnings of actual or latent threats to domestic security, recruiting and training insiders are time-consuming, expensive tasks.

[20] Author interviews, Canberra, October 2007 (see also ASIO, 2006, p. 5; "Australia to Double Spy Personnel," 2005; Head, 2008a).

For this reason, ASIO tends to rely more heavily on community-based information, most of which is obtained from regular interviews with local leaders and representatives.[21] These meetings are conducted under the auspices of the agency's Community Contact Program and are aimed essentially at helping case officers identify and delineate municipal and regional developments that may be relevant to national threat contingencies.[22]

An aggressive, government-run civic outreach initiative complements ASIO's Community Contact Program. Integral to this effort is a National Security Public Information Program, which both explains the principal components of Australia's CT strategy and provides a conduit for community-derived information in support of domestic intelligence assessments (Burch, 2007, p. 10; PM&C, 2006, pp. 41–42). A dedicated National Security Hotline has also been in operation since 2002. Located in the Protective Security Coordination Centre, this secure phone service operates 24 hours a day, seven days a week, allowing ordinary individuals to report any suspicious or unusual behavior that could be relevant to CT.[23] At the time of this writing, more than 42,000 calls to the hotline had been referred to ASIO; 11,500 were assessed as requiring further investigation.[24]

Apart from insider, community leader, and representative sources, HUMINT is also derived from directly tracking and interrogating suspected terrorists. ASIO generally identifies and questions such persons in conjunction with the AFP, and the process occurs in three phases. First, ASIO is required to request an *authority to investigate*, a statutory license issued by the AG that sanctions covert observation of any individual when there is information to suggest that he or she represents

[21] Meetings take place in declared and undeclared settings. In the former case, an ASIO affiliation is specifically acknowledged; in the latter, it is not.

[22] Author interviews, Canberra, November 2003.

[23] Various checks and vetting controls are in place to ensure that the hotline is not misused to denounce or otherwise attack an individual's character.

[24] Author interviews, Canberra and Brisbane, January 2006 (see also PM&C, 2006, p. 19).

a threat to security.[25] If evidence that the surveillance target is taking concrete steps to perpetrate a terrorist attack or cooperate with a militant organization emerges during the course of the ensuing monitoring, ASIO can then apply for a warrant to exercise *special powers*, including the right to initiate search-and-entry operations, access computer hard drives, install listening devices, and intercept and open mail.[26] These highly intrusive techniques can be employed only against individuals whom the agency has solid grounds to believe are actively engaged in pursuits that threaten national security.[27] In all instances, the special powers have to be initially supported by ASIO's Director-General (DG) and subsequently sanctioned—on an individual basis[28]—by the AG. In most cases, special powers have a mandated tenure of six months, after which an the agency must submit an intelligence report detailing how those powers were used and how they contributed to the investigation in question.[29] Once a suspected terrorist suspect is identified, ASIO is empowered to obtain a *questioning warrant* from a federal magistrate that allows the agency to interrogate the suspect and, if necessary, hold him or her for up to 14 days without charge.[30] This expansion in statu-

---

[25] *Security* is defined broadly, encompassing a spectrum that ranges from terrorism to violent demonstration.

[26] Information procured through special powers is automatically destroyed six weeks after the termination of the surveillance operation unless it is deemed instrumental in securing the future conviction of a suspected terrorist.

[27] This process differs from that of the AFP, which must provide evidence that an individual has committed or is about to commit a crime before invoking its special powers, which must in turn be approved by the Ombudsman (author interview, Canberra, October 2007).

[28] There is no such thing as a basket or umbrella warrant that authorizes a bundle of special powers at one time; each has to be approved individually.

[29] Author interviews, Canberra and Brisbane, October 2007.

[30] These powers are closely modeled on those of the Australian Crime Commission, which has similar quasi-executive authority to order an individual to submit to questioning, and are codified in the Australian Security Intelligence Organization Legislation Amendment (Terrorism) Act. The legislation was first enacted as part of a wider suite of emergency laws introduced by the Howard administration in the aftermath of 9/11 and subsequently modified (in terms of its safeguards and oversight provisions) in 2006. In its current form, the act allows ASIO to question suspected terrorists before a prescribed authority of the state in 8-hour blocks for up to 24 hours (48 hours if an interpreter is required) and hold them for a

tory authority[31]—which will sunset in 2016—effectively gives ASIO a short-term right to interview and preemptively hold suspects[32] even if there is no formal written or oral evidence against them.[33]

Intelligence obtained via communication intercepts is an important adjunct to HUMINT. Information collection of this type is typically conducted under the special powers already discussed and, as such, must be sanctioned by the AG and can be conducted only after a warrant that specifies the exact conditions under which the intrusive technique in question can be used has been issued.[34]

In addition to HUMINT and telecommunication and electronic data, ASIO actively procures intelligence from open sources. A wide variety of unclassified publications and assessments—including academic analyses, media reports, and Internet-based documents—is regularly scanned and summarized. This process augments general understanding of the global and strategic environment and assists in the development of actionable police responses to emerging security threats. ASIO has also stepped up its efforts to actively engage subject-matter experts in analytical think tanks and universities and make its officers available to participate in conferences, seminars, and workshops (Chalk and Rosenau, 2004, p. 36).

---

maximum of 14 days, after which they must be formally charged or released (author interviews, Canberra, October 2007; see also Chalk and Rosenau, 2004, p. 57; PM&C, 2006, p. 29; ASIO, 2006, pp. 42, 45).

[31] It is important to stress that the ASIO Legislation Amendment (Terrorism) Act did not sanction any executive authority for the agency, as actual detentions of suspects have to be executed via the AFP. At the time of this writing, no suspected terrorists had been held for more than 48 hours (author interviews, Canberra, October 2007).

[32] The act applies only to those over the age of 16; in instances in which the individual is over 16 but under 18 years of age, a parent or legal guardian has to be present during questioning. In all cases, suspects have the right to have a lawyer present while being interviewed (author interviews, Canberra, October 2007).

[33] Author interviews, Canberra, October 2007. For more on the ASIO Act, see Senate Legal and Constitutional References Committee, 2002. On the concerns the act raises for civil rights, see Parliamentary Joint Committee on ASIO, ASIS, and DSD, 2002.

[34] Author interview, Canberra, February 2003.

Finally, ASIO relies on intelligence provided by the wider AIC. Most of these data are disseminated via the National Counter-Terrorism Committee and National Threat Assessment Centre (NTAC), each of which provides a central mechanism for sharing information and availing interagency operations. Access to these supplementary sources has been extremely important to developing comprehensive threat assessments for such entities as JI, a group whose primary base of operation lies outside Australia's territorial boundaries but whose evolving actions are generally acknowledged to be directly salient to the country's internal security environment.[35]

Leadership and Human Capital

The bulk of ASIO's executive leadership is made up of senior career intelligence officials. While certain appointments have been made from parallel institutions in the wider AIC, most of the upper administrative bureaucratic echelon consists of professionals selected from within the agency itself. Traditionally, these positions were filled by seasoned intelligence analysts who had risen through the ranks. More recently, however, there has been an explicit shift to fast-tracking recent graduates, especially those with backgrounds in international relations and security studies or fluency in foreign—specifically Arabic, Chinese, Malay, or Bahasa—languages.[36]

Entirely different hiring procedures hold for ASIO's top position, that of the DG.[37] At this level, the practice has been to recruit from the outside. Indeed, since 1949, there has been only one internally appointed DG, Peter Barbour, who served in the role between 1970 and 1975.[38] According to a senior Australian intelligence official, it has become

---

[35] Author interview, Washington, D.C., April 2007.

[36] Author telephone interview, June 2007.

[37] The DG of ASIO is a statutory appointment for five years; there is no formal limit on how many terms a DG can serve.

[38] The Gough Whitlam administration dismissed Barbour on grounds of inefficiency before he finished his term.

more or less convention that the agency be run by an external appointee, mainly to avoid public perceptions that the organization is subject to "old-boy inside trading" and, just as importantly, to help ensure that it does not develop a self-replicating (and possibly self-damaging) bureaucratic structure. The official further asserted that DGs with experience in private management or public-sector policymaking circles provide intelligence agencies with a unique outside perspective that can both supplement and enrich the manner in which the intelligence community interprets and carries out its functional role.[39] During the past decade, the diplomatic service has been viewed as particularly instrumental in this regard, with each of the past three DGs (Paul O'Sullivan, Dennis Richardson, and David Sadlier) having been recruited to ASIO from the Department of Foreign Affairs and Trade.[40]

Management and Process

ASIO activities are managed by the agency's DG, who reports directly to the AG (at the time of this writing, Philip Ruddock) and through him to the cabinet's National Security Committee and Secretaries Committee on National Security (SCoNS).[41] The DG oversees formal branch head (see "Organizational Structure and Funding Patterns," below) and operationally focused meetings, each of which occurs at least once a week, and deals with more-routine daily business and functional corporate issues on an as-needed basis.[42] Section 8 of the ASIO Act gives the DG more-formal responsibility for mapping the agency's strategic direction, deciding on resource issues, and ruling on whether a particular issue should be considered relevant to national security.

---

[39] Author interview, Canberra, October 2007.

[40] Author interviews, Canberra, October 2007.

[41] Author interview, Canberra, November 2003. The National Security Committee and SCoNS are essentially responsible for the executive coordination of domestic intelligence. The former consists of senior policymakers; the latter of departmental secretaries (Burch, 2007, p. 10; PM&C, 2006, p. 8).

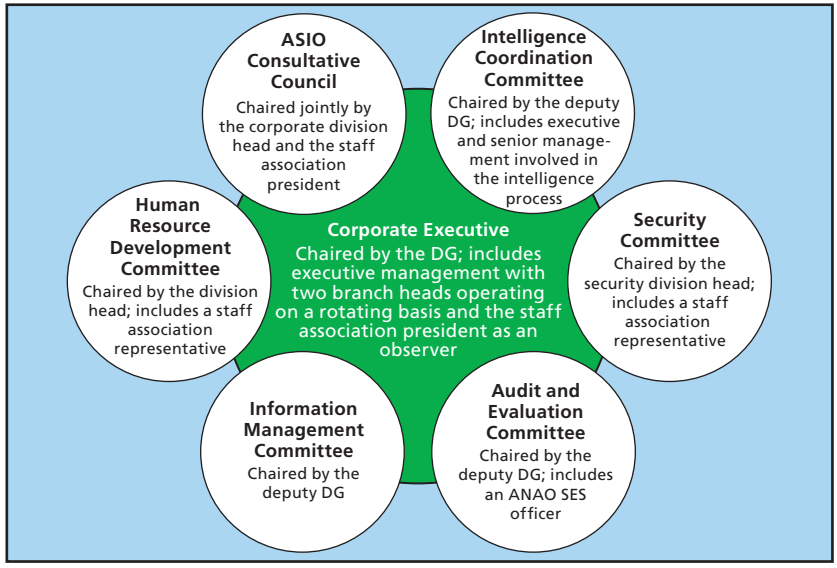
[42] Author interviews, Canberra, October 2007.

These determinations are effectively binding on the agency and they can be overturned by the AG only with the concurrence of the prime minister.[43]

An additional conduit for reviewing ASIO performance and output and ensuring internal transparency and accountability exists in the Executive Council. This corporate body meets every two months and conducts its work through six defined subcommittees (see Figure 2.1):

- the Intelligence Coordination Committee, which reviews Australia's evolving security environment and recommends resource and policy adjustments in response to this changing context

Figure 2.1
ASIO's Corporate Governance Structure



SOURCE: ASIO, 2006. Copyright Commonwealth of Australia. Used with permission.

RAND *MG805-2.1*

[43] Author telephone interview, June 2007. To refute any of the decisions made by the DG, pursuant to Section 8 of the ASIO Act, the AG must do so publicly and must immediately inform the prime minister of the reason for making an adverse ruling of this sort.

- the Audit and Evaluation Committee, which sets the parameters for determining the utility and accuracy of ASIO threat assessments and other internal audits, reviews their outcome, and oversees the implementation of recommendations that flow from these evaluations
- the Information Management Committee, which determines priorities for information-management projects and monitors the manner in which they are put into effect
- the Consultative Council, which provides a structured advisory forum for ASIO management and staff to meet and discuss and resolve outstanding corporate issues
- the Human Resource Development Committee, which provides guidance on staff development and in-house training
- the Security Committee, which is responsible for promoting sound practices and ensuring that they are appropriately considered in all major ASIO developments and initiatives (ASIO, 2007a, pp. 57–58).

Each quarter, all ASIO branch heads are required to submit a performance review to the DG, which, in conjunction with a parallel semiannual assessment of intelligence priorities, forms the basis of the agency's annual report to the federal government. An unclassified version of this document is also made available for open debate in Parliament and for public release in both hard-copy and electronic formats. Together, these reports provide a transparent medium through which the executive and legislative branches can gauge overall ASIO conduct and assess the extent to which ASIO is complying with ministerial guidelines and directives.[44]

Taken as a whole, ASIO's internal corporate governance structure is geared primarily toward ensuring that the DG meets his or her responsibility for the efficient, effective, and ethical use of federal resources by giving added value and direction to domestic security intelligence operations in Australia. Just as importantly, it is designed to provide an objective basis for mitigating risk, determining and eval-

[44] Author interviews, Canberra, October 2007.

uating performance vis-à-vis internal priorities, and ensuring business continuity across each of the agency's core functional divisions.

For the most part, ASIO has undertaken its internal intelligence function in accordance with the stated objective of employing surveillance and analytical assets in the most cost-effective manner possible. However, there have been occasions when this goal has clearly not been achieved. A graphic case in point concerns the investigation into Mohammed Haneef, an Indian Muslim doctor who was implicated in a series of failed bombings directed against nightspots in London and Glasgow International Airport in 2007. The investigation, which ultimately failed to produce any credible evidence against Haneef, involved dozens of officers working in conjunction with the AFP to carry out search warrants, intercept telephone calls, and trawl computer hard drives. More than 300 witness statements were taken, 349 forensic samples were collected, and 623 gigabytes of electronic data were seized. The final bill for what was essentially an intelligence effort mounted against a single individual included A$1.6 million in overtime and eventually totaled more than A$7.5 million (Head, 2008).

Organizational Structure and Funding Patterns

ASIO's organizational structure provides clear points of focus for conducting specific intelligence tasks, satisfying related customer requirements, and ensuring that all relevant logistical and administrative priorities associated with managing the day-to-day running and future growth of the agency are covered. As Table 2.1 delineates, this framework is split across eight functionally specific branch divisions (plus an additional management division).

Key Relationships with Other Intelligence and Law Enforcement Agencies

The Australian Intelligence Community

ASIO enjoys well-established working, liaison, and information-exchange relationships with key partners in the wider AIC. These

Table 2.1
ASIO Organizational Structure, 2007

Division	Subdivisions
Investigative Analysis and Advice	Middle East and Africa Australia, Pacific, Asia, Europe, and Americas Counter-Terrorism Litigation Advice Leads, Events, and Counter-Proliferation
Strategic Intelligence and Liaison	NTAC Strategic Analysis International Engagement and Reporting
Collection	New South Wales Victoria Central Resource Coordination
Counter-Espionage and Foreign Interference	Counter-Espionage Foreign Interference
Technical Capabilities	Telecommunications Technical Operations Surveillance
Security	Counter-Intelligence and Security Protective Security Security Assessments
Information	Information Capability Development Information Capability Provision Information Services
Executive and Legal	Legal Advice Litigation Executive
Corporate Management	People Finance Property

SOURCE: ASIO, 2007a, pp. 12–13.

include the following six main agencies, all of which have a remit, to varying degrees, to engage in CT information collection and analysis:

- the Australian Secret Intelligence Service (ASIS), which is responsible for gathering secret information about the intentions, capabilities, and activities of individuals and organizations outside

Australia that might affect the country's strategic standing or security interests
- the Defense Intelligence Organisation, which is responsible for assessing intelligence pertinent to global security developments, defense economics, and any science and technology applications that could be used for military purposes
- the Defense Signals Directorate (DSD), which acts as Australia's primary national signals intelligence (SIGINT) agency responsible for communication intercepts and safeguarding the integrity of the country's information systems
- the Defense Imagery and Geospatial Organisation (DIGO), which supports federal national security efforts and Australian Defence Force operations through the collection and analysis of imagery and geospatial data
- ONA, which provides strategic assessments and forecasts to the Department of the Prime Minister and Cabinet (PM&C) as well as other senior policymakers in the federal government on key international, political, and economic developments that are salient to Australian interests at home and abroad (PM&C, 2006, pp. 31–33).

Interaction with these agencies is availed primarily through NTAC, which was set up in 2004 to provide single-voice assessments for Australian CT. The center includes seconded officials from ASIO, ASIS, ONA, the AFP, the Department of Transport and Regional Services; and the Department of Foreign Affairs and Trade. A Terrorist Threat Advisory Group consisting of delegates from each of the participating agencies as well as an official from PM&C meets at least weekly to ensure effective coordination in preparing and disseminating forecasts for determining broad national CT alert levels,[45] risks to

[45] There are four national CT alert levels in Australia: *low* means that a terrorist attack is not expected; *medium* means that a terrorist attack could occur; *high* means that a terrorist attack is likely; *extreme* means that a terrorist attack is imminent or has occurred (author interview, Canberra, November 2003).

specific events and people, and threats to Australian interests at home and overseas.[46]

Another important forum is the Joint Counter-Terrorism Intelligence Coordination Unit (JCTICU), which was established in 2002 to enhance collaboration between police and intelligence agencies, particularly in terms of helping to ensure that security information procured from across the AIC is quickly translated to assist law enforcement CT investigations on the ground. The unit includes representatives from ASIO, DSD, DIGO, and the AFP and is overseen by a steering committee (chaired by ASIO's DG), which sets its overall strategic direction.[47]At a broader policy level, ASIO's links to the wider AIC occur as a natural by-product of their common representation on the National Counter-Terrorism Committee (NCTC). Created in October 2002 to act as a high-level decisionmaking and coordinating body, the committee acts as a central vehicle for effective policy development and integration of national CT initiatives and information. It maintains the National Counter-Terrorism Plan, which outlines responsibilities, authorities, and mechanisms to prevent terrorist attacks and manage their consequences within Australia.[48] NCTC works closely with the Protective Security Coordination Centre Watch Office, which again includes cross-agency representation from the intelligence and federal law enforcement communities and integrates and fuses information flows—on a 24/7 basis—between commonwealth, state, and territory governments on national security issues (PM&C, 2006, p. 15).

---

[46] Author interviews, Canberra, November 2003, January 2006, and October 2007 (see also PM&C, 2006, p. 31; AG, 2003; Burch, 2007, p. 9).

[47] Author telephone interview, June 2007; AFP, 2006, p. 22.

[48] NCTC was established to integrate and rationalize the work of the Standing Advisory Committee on Commonwealth/State Cooperation for Protection Against Violence and its counterpart, the Special-Interdepartmental Committee on Protection Against Violence, and reports annually to the Council of Australian Governments, which acts as Australia's principal intergovernmental policy forum for starting, developing, and monitoring the implementation of initiatives, both security and nonsecurity, that are of national significance.

Law Enforcement

ASIO maintains a close and effective working relationship with the law enforcement community in Australia. The principal point of contact is the AFP, which is responsible for combating crime that has a specifically national dimension.[49] However, because the AFP retains the national perspective on policing in Australia, it also acts a primary conduit for expediting ASIO links to police forces in each of the country's state and territory jurisdictions.[50]

In many ways, ASIO-AFP interaction is a product of trust and personal relationships that have evolved over time and that reflect the relatively small size of the Australian intelligence and law enforcement communities.[51] While inevitable sensitivities persist over the appropriate dissemination of classified material—particularly the question of how or when it should be used to secure criminal prosecutions[52]—the organizations tend to view CT in largely similar terms and generally agree that it is a functional priority that necessarily has to be jointly owned.[53]

---

[49] AFP, 2006, p. xi. In 2003, the AFP adopted a functional organizational structure to address crimes that carry direct implications for national security. At the time of this writing, these were defined as terrorism and drug trafficking, the force's two main priority areas, as well as money laundering, illegal migration, cyber-crime or electronic crime, and major fraud (author interview, Washington, D.C., April 2007).

[50] Author interview, Washington, D.C., April 2007.

[51] Author telephone interview, June 2007.

[52] Author interviews, Canberra, October 2007. ASIO, in common with many security intelligence agencies around the world, continually confronts the challenge of how to securely disseminate classified information for evidentiary purposes without unduly exposing the identity of covert intelligence sources and practices. In an effort to overcome this issue, the Australian government has authorized the initiation of a high-level working group to study the feasibility of setting up a platform to avail the secure dissemination of top-secret information among ASIO, law enforcement, and the wider AIC. At the time of this writing, a blueprint for such a conduit had been developed, although no working model had actually been tested or implemented.

[53] Author interview, Washington, D.C., April 2007. The AFP's undercover policing program (Axiom) is closely integrated with the force's intelligence function, ensuring that information received through undercover sources is able to support other covert surveillance and monitoring activities.

Integral to the AFP-ASIO working relationship has been the development of formal institutional processes to avail the linear exchange and analysis of covert information and to expedite combined operations. As noted in the earlier section dealing with "Mission and Critical Capabilities," the AFP and ASIO are engaged in concerted efforts to counter CBRNE terrorism through their joint participation in SWAG. The federal police also enjoy permanent representation in NTAC and JCTICU.[54] Seconding AFP officers to these two bodies, both of which are housed at ASIO headquarters in Canberra, has two main benefits:

- It has ensured the timely integration of pertinent, police-specific information into wider national security intelligence assessments.
- It has helped generate actionable CT intelligence by providing a conduit through which relevant investigative and operational opportunities identified at the street level can be pursued (AFP, 2006, p. 22).

Besides SWAG, NCTC, and JCTICU, formal AFP-ASIO institutional ties occur through the National Intelligence Group, the Joint Intelligence Group, and Police Forward Command Posts. These forums are designed primarily to coordinate and disseminate intelligence support to operational commanders at the scene of a terrorist attack (ASIO, 2005, p. 38). According to officials in Australia, these response structures have provided an effective conduit through which relevant classified material can be imparted to help assist with postincident investigations and consequence management.[55]

Finally, effective organizational and operational links have evolved through regular cross-agency exchanges and training programs. Established liaison arrangements between ASIO and the AFP, which are not statutorily required, now take the character of semipermanent secondments. Several police-designed modules are also in place to heighten awareness among intelligence personnel of such issues as evidence han-

[54] Author interviews, Canberra, October 2007. At any one time, there will be two AFP officers assigned to NCTC and one to the JCTICU.

[55] Author interviews, Washington, D.C., April 2007, and Canberra, October 2007.

dling and collecting security information in a manner that will maximize its prosecutorial value. By the same token, ASIO runs numerous in-house seminars for law enforcement to explain the agency's work and role and to impart a more sophisticated understanding of evolving terrorist dynamics and their relevance to Australian national security interests.[56]

This two-way exchange and training commitment is supplemented by a national exercise program designed to ensure that standing collaborative arrangements between the police and intelligence communities—and other key CT stakeholders—are well-practiced and validated. One of the largest simulations to date took place in October 2005. Code-named Mercury 05, the drill was designed to test national security arrangements for the Melbourne 2006 Commonwealth Games and was, according to one senior AFP official, highly instrumental in forging extremely close functional ties between ASIO, the AFP, and Victoria law enforcement.[57] At the time of this writing, the federal government had allocated some A$28 million to further refine and develop the exercise program through 2011.[58]

Oversight

In addition to internal corporate management, ASIO operates under a comprehensive external oversight and control regime to ensure that it works strictly within statutory limits in performing its roles and functions. Two principal bodies are integral to this framework: the AG's

---

[56] Author interviews, Canberra, October 2007; ASIO, 2006, p. 44.

[57] Author interview, Washington, D.C., April 2007.

[58] PM&C, 2006, p. 15; ASIO, 2006, p. 49. Mercury 05 involved large-scale deployment activities and more than 4,000 participants from Victoria, South Australia, Western Australia, New South Wales, the Australian Capital Territory, and the federal government. For further details on the exercise, see Attorney-General's Department, "Mercury '05: Questions and Answers," Web page, undated.

Inspector-General of Intelligence and Security (IGIS) and the Parliamentary Joint Committee on Intelligence and Security (PJCIS).[59]

IGIS has extremely wide-ranging powers and enjoys access to all organizational staff and documentation, including that pertaining to active operations. At the request of a minister or in response to complaints from the general public, the IGIS may inquire independently into matters concerning ASIO legal compliance and propriety. Abridged outcomes of these investigations are compiled in a report that is tabled before Parliament each year.[60] IGIS reviews of ASIO activity are extensive and can address any of the following substantive material or concerns:

- operational cases and files
- use of intrusive or special powers requiring a warrant
- compliance with the 1983 Archives Act[61]
- access to and use of financial information obtained from the Australian Taxation Office and the Australian Transaction Reports and Analysis Centre (AUSTRAC)[62]
- providing information to and liaising with law enforcement

---

[59] Besides IGIS and PJCIS scrutiny, ASIO financial records and systems are subject to annual review by the Australian National Audit Office (ANAO). In addition, the AG can issue guidelines that elaborate on ASIO's legislative framework in terms of what the agency can and cannot do, while qualified and adverse ASIO security assessments may be lodged for appeal with the Security Appeals Division of the Administrative Appeals Tribunal (AAT) (author telephone interview, June 2007). Further details about the investigatory role of the ANAO and AAT can be obtained from AAT, undated, and ANAO, undated.

[60] Author telephone interview, June 2007, and Canberra, October 2007; Burch, 2007, p. 10; PM&C, 2006, pp. 41–42.

[61] Although ASIO is exempt from the provisions of the Freedom of Information Act (1982), it is required to abide by the Archives Act, which allows members of the public to access agency records that are at least 30 years old. In general, release of these data is denied only when disclosure could damage national security or expose the existence or identity of a confidential source.

[62] AUSTRAC acts as Australia's main anti–money-laundering regulator and financial intelligence unit. Domestically, AUSTRAC provides monetary-transaction reports and other fiscal data to federal, state, and territory law enforcement and revenue agencies; internationally, it works to facilitate the exchange of financial information for combating money laundering, organized crime, revenue evasion, and terrorism financing (PM&C, 2006, p. 36).

- official use of alternative documentation to support assumed identities (ASIO, 2006, p. 61).

An important feature of IGIS scrutiny lies in IGIS's ability to conduct real-time investigations into ongoing ASIO operational activities. This power ensures that IGIS's oversight function is not merely ex post facto in nature but can be initiated any time that some form of transgression is suspected or otherwise judged to have taken place.[63]

The PJCIS (formerly known as the Parliamentary Joint Committee on ASIO, ASIS, and DSD) was established in September 2001 as part of the Intelligence Services Act.[64] The committee's role is to provide legislative oversight of the AIC and it is mandated to conduct investigations into virtually all aspects of ASIO administration and expenditure. It can request evidence and briefings from the agency's DG and case officers, but it cannot request material that is either operationally sensitive or relates to active intelligence-gathering priorities.[65] PJCIS reviews must be undertaken at least once a year and, because independent lines of inquiry can be initiated at any time, they are not contingent on requests from outside third parties (PM&C, 2006, p. 33; ASIO, 2006, p. 60; Chalk and Rosenau, 2004, pp. 40–41).

Performance Metrics

ASIO has yet to develop a rigorous system for evaluating the efficacy of its functional activities. In common with many CT security agencies around the world, the tendency has been to default to measurements of *output* rather than *outcomes*: That is, the metrics describe measures that

---

[63] Author interview, Canberra, February 2003.

[64] PJCIS replaced and greatly expanded on its successor organization, which was created in 1988 with only limited powers of external intelligence oversight. Prior to 1988, there was no formal legislative scrutiny over any aspect of the AIC.

[65] Author interviews, Canberra, October 2007; Burch, 2007, p. 10; PM&C, 2006, p. 42. It should be noted that PJCIS's remit also excludes reviews of individual complaints, all of which are the exclusive domain of the IGIS.

have been put in place as opposed to assessing how effective individual modalities have been.[66]

That said, ASIO has implemented a basic system for gauging performance, much of which is based on external feedback and comments on its principal products from external customers. Each year, the agency conducts a survey of its main commonwealth, state, and territory clients, the results of which are included in the annual report provided to the federal government and Parliament. Customers are asked to rank ASIO advice and quality of analysis according to one of the following four rankings: almost always useful, generally useful, sometimes useful, or rarely useful.[67] In 2006, roughly 98 percent of ASIO's commonwealth clients rated the agency's product as either almost always or generally useful (ASIO, 2005, p. 11). This figure largely accords with results from the previous two years, the details of which are displayed in Table 2.2.

ASIO performance is also assessed against the total price of its product output. The Audit and Evaluation Committee undertakes these audits, the results of which are documented in detail in ASIO's classified annual report.[68] They also form a key element of PJCIS's oversight function and the Australian National Audit Office's (ANAO's) statutory responsibility to review ASIO's financial records and systems.

Finally, ASIO frequently relies on various procedural aspects of its internal governance structure to assess the agency's overall performance. Of particular importance in this regard are the meetings of the Executive Council (which are held twice a month), the performance review that all branch heads are required to provide each quarter, and the termination-of-intelligence reports that are a necessary component of all special-power authorizations.[69]

---

[66] Author telephone interview, June 2007. As one intelligence official remarked, "Measuring counter-terrorism is extraordinarily difficult; I don't think any country has come up with a satisfactory system for evaluating performance that does rely on outputs."

[67] Author interviews, Canberra, October 2007.

[68] Author interviews, Canberra, October 2007.

[69] Author interviews, Canberra, October 2007.

Table 2.2
ASIO Client Survey Results, 2003–2005

	Response (%)							
	Almost Always Useful		Generally Useful		Sometimes Useful		Rarely Useful	
Client	2003–2004	2004–2005	2003–2004	2004–2005	2003–2004	2004–2005	2003–2004	2004–2005
Commonwealth	62.4	68.0	29.3	31.0	8.3	1.0	0	0
Police	66.5	57.0	29.0	40.0	4.5	3.0	0	0
Total (average)	64.5	62.5	29.2	35.5	6.4	2.0	0	0

SOURCE: ASIO, 2005, p. 11.

Problems or Controversies

Periods of abuse and crisis that have significantly affected ASIO occurred primarily during the agency's early history and, for the most part, revolved around scandals pertaining to Soviet infiltration and illegitimate surveillance of left-wing activists. The general issue of communist subversion in Australia has been the subject of at least three concerted Royal Commissions: the Royal Commission on Espionage (1954–1955),[70] the Royal Commission on Australian Security and Intelligence Agencies (1983–1984),[71] and the Inquiry into National Security (1993). Of these, it is the third that is most pertinent to ASIO. The commission, instituted under the auspices of Michael Cook (a former head of the ONA), was established following the trial of George Sadil, a Komityet Gosudarstvennoy Bezopasnosty [Committee for State Security] (KGB) mole who had managed to penetrate and work in ASIO as a Russian interpreter for 25 years.[72] The review, completed in 1994, recommended several changes to the agency's internal vetting procedures for individual access to highly classified material.

ASIO has also been the subject of several controversies concerning supposed surveillance of legitimate opponents and critics of the

---

[70] The Royal Commission on Espionage was established in May 1954 to inquire about the intelligence activities of foreign governments on Australian soil. It was formed following the highly publicized defection of Vladimir Mikhaylovich Petrov, the third secretary at Moscow's diplomatic mission in Canberra. His revelations helped expose an entrenched spy network that had, for several years, based itself out of the Soviet Embassy and that eventually proved instrumental in leading to the expulsion of several Soviet diplomats accused of violating their positions to the detriment of Australia's national security interests. For further details, see NAA, 2006.

[71] This commission was established following the expulsion of Valeriy Ivanov, first secretary at the Soviet Embassy in Canberra, on grounds of subversion and espionage. It recommended that the security-related activities investigated by ASIO be redefined and that the agency be given additional responsibilities for foreign intelligence collection in Australia (see RCASIA, 1985).

[72] The AFP arrested Sadil in June 1993, finding him in possession of highly classified documents that he later admitted in court had been removed "contrary to his duty" as an ASIO officer. Sadil was sentenced to three months in jail but was subsequently released on a 12-month good-behavior bond. For two interesting accounts of the affair, see "ASIO Mole Sold Secrets to KGB," 2004, and Hardaker, 2004.

government. This was particularly true during the 1950s and 1960s, when there were numerous allegations that the agency was actively engaged in targeting the political left, including senior members of the Labour Party;[73] writers, actors, and artists with socialist tendencies; and anti–Vietnam War protesters. Certain assertions went even further and, in one notable instance, extended to an accusation that ASIO had compiled a list of some 10,000 communist sympathizers who would be immediately rounded up and interned in the event of an escalation in the Cold War (see "War on Dissent," undated). Questions raised by these contentions eventually resulted in an extensive three-year review (1974–1977) of security and intelligence operations in Australia. Conducted under the auspices of Justice Robert Hope of the Supreme Court of New South Wales, this assessment was directly responsible for much of the accountability framework that has since been such an integral feature of the agency's overall organizational structure.[74]

Besides these general areas, a number of specific cases have had varying degrees of significance for the credibility and perceived effectiveness of domestic intelligence in Australia. In 1973, AG Lionel Murphy accused ASIO of failing to pass on relevant intelligence that could have helped prevent a far-right-wing Croatian militia from carrying out a series of bombings against the Yugoslav consulate in Canberra.[75] Five years later, the agency was directly linked to the terrorist attack on the Sydney Hilton, and one former police officer, Terry Griffiths,[76] claimed that the strike had been deliberately allowed to go ahead in order to justify an increase in ASIO's operational budget and powers. In 1982, a highly publicized court filing was brought against the AG contending

---

[73] In one notable case during the 1950s, circumstantial links were noted between the head of the Labour Party and the Communist Party of Australia (and, hence, to the Soviet Union).

[74] Author telephone interview, June 2007.

[75] It should be noted that the AG was a member of the recently sworn-in Labour Government, which still harbored a deep-seated suspicion of ASIO because of its surveillance activities during the 1950s and 1960s. Murphy ordered a raid on the agency's central office in March 1973, which proved disastrous and failed to provide any evidence in support of his claims.

[76] Griffiths was one of the eight people injured in the explosion. For an interesting account of the attack and the various theories surrounding who was behind it, see O'Brien, 2003.

that he was orchestrating a deliberate attempt to destroy the Church of Scientology by portraying the organization as a dangerous cult that posed a clear threat to Australian national security.[77]

Finally, ASIO has been the subject of at least three highly publicized scandals that occurred in the context of heightened, post-9/11 terrorism concerns. The first case, a relatively minor one, took place a few weeks after 9/11, when ASIO broke into what it thought was the house of a suspected jihadist terrorist by the name of Bilal Daye. Subsequent investigations revealed that the search warrant authorizing the raid was for a different address.[78]

More serious was the investigation—discussed above under "Management and Process"—into Mohammed Haneef, who was implicated as a material accomplice in the attempted bombings of two central London nightclubs and Glasgow International Airport in 2007.[79] Haneef, who was a distant cousin of a man involved in the attacks, Kafeel Ahmad, was arrested in Brisbane as he was leaving Australia on a one-way ticket to India. He was held without charge for two weeks amid claims that he was part of a "global terror network" engaged in conducting and planning attacks against Western interests. The sole evidence used to detain the doctor was a cell phone subscriber identity module card (better known as a SIM card) found in a Jeep that exploded outside Glasgow Airport, and which authorities claimed Haneef had given to Ahmed's brother in 2006. The case was dropped after federal prosecutors admitted that they had made erroneous statements concerning the mobile phone based on false information they had received from the AFP and ASIO.[80]

---

[77] The court injunction was dismissed, and the case never went to trial.

[78] Daye subsequently sought damages from the government, and the embarrassing incident was settled out of court in 2005. All material relating to the case has subsequently been designated "strictly confidential." See "Couple Wins Payout Over ASIO, AFP Raid," 2005.

[79] For more on the planned attacks, see Stewart, 2007, and Cowell and Bonner, 2007.

[80] Head, 2008b; Bonner, 2007; Johnston, 2007; Maley, 2008. Although Haneef was initially granted bail by a Queensland judge (largely because the evidence against him was so flimsy), Immigration Minister Kevin Andrews immediately suspended his visa, which allowed the government to hold him in indefinite administrative detention. Once the case

Later that same year, ASIO became embroiled in a third controversy, this time involving a student who had been accused of attending a terrorist training camp run by the Army of the Pure, a militant group based in Pakistan, in early 2003. The individual, Izhar ul-Haque, was formally arrested in April 2004 on the basis of a confession given to intelligence agents six months earlier. He was charged with one count of terrorism and kept in solitary confinement for half a year before being granted bail. However, the case was dropped in 2007 after the Supreme Court of New South Wales ruled that ul-Haque had been illegally detained and questioned by ASIO officers who had, in effect, themselves broken the law. The presiding judge was unambiguous in his closing remarks:

> It was a gross interference by the agents of the state with the accused's legal rights as a citizen, rights he still has whether he be suspected of [illicit] conduct or not and whether he is Muslim or not. . . . I am satisfied that [agents] B15 and B16 committed the criminal offenses of false imprisonment and kidnapping.[81]

Conclusion

Since its creation in 1949, ASIO has developed into a mature and complex organization that currently represents Australia's main weapon for countering terrorist threats to the country's national security, whether they emanate from external or internal sources. The agency has steadily expanded in tandem with the contingencies of the post-9/11 era and is expected to have an operational staff of around 1,860 by 2010–2011. In carrying out its domestic surveillance mandate, ASIO is subject to

---

was dropped, the federal court ruled that Andrews's revocation order was illegal; Haneef then voluntarily left Australia and returned home to Bangalore.

[81] See Johnston, 2007. ASIO detained ul-Haque in November 2003 on the basis of a "simple" search warrant. Despite the limited scope of this executive order, ul-Haque was bundled into a car, driven to a park, and threatened with "adverse consequences" unless he cooperated. He was then taken home and interrogated in his bedroom for several hours before finally being released.

routine executive and legislative oversight, has not been granted any independent arrest authority (any limited detention powers have to be instituted through the AFP), and has been explicitly obligated to demonstrably justify the need for highly intrusive techniques (which must be judicially sanctioned and renewed on an individual basis). Moreover, because terrorism has been mainstreamed as a core issue in Australia, ASIO has necessarily been required to interact and liaise with other government agencies and the private sector. Toward that end, dedicated coordinating mechanisms have been established to link the agency with law enforcement and the wider intelligence community, and nascent but increasingly robust partnerships now link ASIO with industry and business representatives.

The ASIO case provides a good example of how a liberal democratic state has sought to balance the need for security in the common name with the equally important imperative of defending and upholding individual rights and freedoms. While by no means blemish free, the agency's overall track record has been largely devoid of major controversies and scandals—a fact that reflects the success of the intricate set of statutory safeguards and controls that have explicitly accompanied the agency's operation. Managing ASIO's work in this manner has provided a transparent means of assessing and evaluating the utility of the covert intelligence function, which has ensured necessary accountability at the government level and helped to mitigate against a general loss of trust and confidence among the public as a whole.

CHAPTER THREE

Canada

Peter Chalk

Canada has been largely free of indigenously based terrorism in recent years, with the main manifestations of current domestic political extremism arising from the activities of neo-Nazis and violent fringe elements of ecological, animal-rights, and antiglobalization movements. However, the country has been decisively affected by the spillover effects of overseas conflicts and continues to act as a highly important hub of political, financial, and logistical support for Sikh and Islamic radicalism as well as ethnonationalist separatist movements originating in the Middle East, Central and South Asia, and Africa (CSIS, 2005a, p. 5; CSIS, 2007b, p. 6).

With the possible exception of the United States and the United Kingdom, Canada has played "host" to more international terrorist organizations than any other state in the world. Indeed, in the past decade, "representatives" of Hamas, Palestinian Islamic Jihad, the Groupe Islamique Armé [Armed Islamic Group] (GIA), al Qaeda and its affiliates, the Provisional Irish Republican Army, the Liberation Tigers of Tamil Eelam (LTTE), the Partiya Karkerên Kurdistan [Kurdish Workers' Party] (PKK), Babbar Khalsa, and the Dashmesh Regiment are all known to have entered the country and engaged in a variety of lobbying, fund-raising, and other logistical-support pursuits.[1] It is toward the mitigation of these activities that the bulk of Canada's CT

[1] To a large extent, this situation results from the fact that the state, which has been founded on a commitment to immigration and ethnonational and religious tolerance, represents a source of political refuge that has been effectively exploited by extremist elements from around the globe.

intelligence effort has been, and continues to be, directed—although, as in Australia, it is the threat of al Qaeda–inspired or related Sunni and Shi'a Islamic extremism that remains the main concern.[2]

Creation and Relevant History

Responsibility for domestic intelligence in Canada falls to the Canadian Security Intelligence Service (CSIS), which was created by an act of Parliament (Bill C-9) on June 21, 1984.[3] Prior to this, sole responsibility for internal surveillance lay with the Royal Canadian Mounted Police (RCMP) Security Service. Following the Royal Commission of Inquiry into Certain Activities of the Royal Canadian Mounted Police (the McDonald Commission) in the late 1970s, however, it was decided that vesting responsibility for intelligence in the hands of a police body that retained full executive powers of arrest and detention was contrary to the democratic ethos that underscored the Canadian way of life. More specifically, there were fears that, if left unchecked, the RCMP could degenerate into a rogue agency under which the pretext of "national interest" would be used to justify the covert monitoring and detention of legal political entities. It was thus decided to create an entirely new, civilian organization—CSIS—that would have no functional law enforcement authority and that would have a solid legal basis that mandated a rigorous system of internal and external democratic oversight and control.[4]

---

[2] Author interview, Washington, D.C., June 2007 (see also SIRC, 2006, p. 39; CSIS, 2005a, p. 1).

[3] CSIS began its formal existence on July 16, 1984.

[4] Author interview, Washington, D.C., May 2007 (see also CSIS, 2005b, p. 1). It is interesting that the exact same logic that led to the creation of CSIS was used by the United States to keep both police and intelligence functions within the FBI following the abuses of the Hoover era. In the latter case, it was argued that control of internal surveillance would be better served by limiting the statutory power of an overt federal law enforcement institution than by creating a separate, covert agency whose sole mission lay in the realm of domestic spying.

Mission and Critical Capabilities

CSIS is empowered to forewarn and advise the government through the provision of timely and accurate information about activities that may constitute a direct threat to the domestic security of Canada. At its inception, the bulk of the service's activity was directed at countering espionage and foreign-influenced activities, and this mission consumed as much as 80 percent of the service's resources. The growing complexity of extremist political violence since the end of the Cold War, ongoing conflicts in Asia and the Middle East, the emergence of a global jihadist network affiliated with or inspired by al Qaeda, and Canada's own forward role in support of U.S.-led military incursions into Afghanistan and Iraq have fundamentally altered CSIS's priorities, with CT now constituting the agency's chief focus. This is true in terms both of mitigating attacks in Canada and preventing the country's territory from being exploited as a logistical base in or from which to plan, prepare, and launch strikes elsewhere.[5]

Like Australia's ASIO, CSIS has increasingly viewed this mission statement as one that necessarily requires an explicit foreign component—especially given the fact that the country lacks an external intelligence bureau. As one official remarked to the author, CSIS

> can no longer afford to think of itself as purely domestic in nature. The character of the contemporary transnational terrorist phenomenon has shifted the operational focus of the agency, which

[5] CSIS's most recent annual report is categorical about the salience that PMV holds for the state's overall national security interests and highlights the following six factors as issues of particular concern: (1) persons trained in terrorist training camps and veterans of campaigns in Bosnia, Chechnya, Afghanistan, Iraq, and elsewhere are known to reside in Canada; (2) Canadians who have traveled to Iraq to fight against coalition forces in the Iraqi insurgency may return home with new skills and new motivations; (3) a relatively large number of religious, separatist, and ethnonationalist terrorist groups are known to be operating in Canada and engaged in fund-raising, procuring materials, spreading propaganda, recruiting followers, and other activities; (4) terrorist groups continue to intimidate and exploit Canada's immigrant and expatriate communities, sometimes through front organizations; (5) Canadian residents and citizens are known to have planned operations against foreign entities and to have personally participated in them; and (6) terrorists in Canada have conducted reconnaissance against potential terrorist targets (see CSIS, 2005a, p. 2).

> is now far more international in orientation. You can't investigate threats from the Middle East and Asia by staying in Canada.[6]

This shift has had implications for the agency's organizational structure (discussed below).

In working to counter the terrorist threat to Canada, CSIS engages in a thorough intelligence-collection effort that spans the spectrum of SIGINT to HUMINT. Data originate from many principal sources, including the following: general covert observation operations; more-intrusive special investigation techniques—such as electronic (video) surveillance, bugging and wiretapping of private communications, intercepting and opening mail, installing tracking devices, taking DNA samples, and covert search and entry operations—that must be approved by a federal court affidavit (discussed later); the wider Canadian intelligence community (CIC);[7] open-source academic research (especially that which pertains to specific extremist groups or global trends); and interviews with terrorist insiders, plea bargainers, and immigrant community leaders and representatives.[8] This information forms the basis of regular strategic and tactical threat assessments, which are designed to provide time-sensitive evaluations of the imme-

---

[6] Author interview, Washington, D.C., June 2007. Foreign intelligence activities undertaken by CSIS are authorized under Section 12 of the service's creation act, which generally sanctions covert surveillance of threats to Canadian national security (although more-traditional, narrowly focused spy work can be undertaken only within Canada), and, for the most part, are performed by dedicated senior liaison officers stationed in Canada's principal embassies and overseas diplomatic missions.

[7] Principal members of the CIC include the Department of National Defence (DND); the Communications Security Establishment, Canada's equivalent of the U.S. National Security Agency (NSA); the Department of the Solicitor General; Public Safety and Emergency Canada; Transport Canada; Citizenship and Immigration Canada; the Canada Border Services Agency (CBSA); the Department of Foreign Affairs and International Trade Canada; and the RCMP.

[8] CSIS runs an extremely active outreach program with community leaders and representatives, both as a means of collecting intelligence and as a way of giving the service more of a public face by explaining to the average individual what the agency actually does (author interview, Washington, D.C., June 2007).

diacy and scope of terrorism-related threats to Canada and Canadian interests.[9]

Security intelligence is also fused with information drawn from the wider CIC to form holistic, single-voice CT assessments generated in the Integrated Threat Assessment Centre (ITAC). Established in 2004 and similar to NTAC, its Australian counterpart, this body acts as a 24/7 emergency assistance and management community resource that operates under the auspices of the National Security Policy. It carries and out distributes risk-vulnerability appraisals that are undertaken at its own behest; in response to specific requests from third-party customers; or in preparation for major political, public, or international events (CSIS, 2005a, p. 14; SIRC, 2006, pp. 9–10).

Another principal recipient of CSIS intelligence—in this instance, derived from the service's Immigration Threat Assessment Unit—is the Enforcement Information Index located in CBSA. Federal authorities use this database to issue alerts whenever known or suspected terrorists or sympathizers seek to enter the country under the guise of being short-term visitors, long-term immigrants, or asylum-seekers (CSIS, 2002, pp. 8–11; SIRC, 2006, p. 39).

Finally, through the generation of security intelligence reports, CSIS directly contributes to the central government's terrorist-entity listing process. These written assessments describe the grounds for designating a particular organization or individual as a threat to national security and help the Minister of Public Safety and Emergency Preparedness (PSEP) determine whether to recommend to the Governor in Council that a particular entity be duly proscribed.[10] Security intelligence reports are also used in the service's consultations with Foreign Affairs Canada in listing the names of persons or groups under Schedule 1 of the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism (SIRC, 2006, pp. 40–41).

---

[9] Author telephone interview, May 2007.

[10] More information on this process and the entities included on the list can be found at Public Safety Canada, undated.

Like ASIO, CSIS performs an important role in terms of four types of domestic security screening.[11] First, the service vets the backgrounds of individuals who require authorization to access particular forms of sensitive data.[12] As Table 3.1 shows, the median turnaround time for these evaluations depends on the level of clearance required and the source of the requesting agency or department; for DND, processing times in 2005 and 2006 ranged from 24 days for confidential (Level I) to 39 days for top secret (Level III).[13]

Second, CSIS determines the legitimacy of individuals applying for citizenship, permanent residence, or refugee status. The service received 400,000 such requests between 2005 and 2006 and prepared 469 briefs (assessments) in response to these petitions; 232 of these responses were information briefs and 117 were inadmissibility briefs (see Table 3.2).[14]

Third, the agency assesses the threat potential of resident foreign nationals who have come to authorities' attention because they may pose a risk to the national security of Canada (CSIS, 2005a, pp. 3, 13–14).

---

[11] Occasionally, CSIS will supply security assessments of individuals to foreign states and international agencies and organizations (such as the International Criminal Police Organization, better known as INTERPOL) under reciprocal screening agreements. Generally, the service becomes involved in this type of activity only if an overseas government requests that it do so (for instance, if a Canadian citizen seeks residence in another country) or if it receives information of concern from an established source.

[12] The largest clients of this service are Public Works and Government Services Canada and DND, which, combined, accounted for 45 percent of all security-clearance requests between 2005 and 2006. CSIS does not vet Canada's national police force; that responsibility falls directly to the RCMP. Note, however, that the service does provide assessments for the Mounties on an as-needed or as-requested basis.

[13] Security assessments are conducted under the authority of Sections 13 and 15 of the CSIS Act.

[14] An *information brief* is usually issued when there is some question about an applicant's background that could be grounds for inadmissibility; the brief sets out these concerns, assesses their validity, and recommends a tentative course of action for the government. An *inadmissibility brief* that recommends against allowing the individual to enter the country is generally made in response to immigration or asylum requests from individuals who are somehow connected to a proscribed terrorist entity or hostile intelligence service. All reviews of citizenship and permanent-residence applications are conducted under Sections 14 and 15 of the CSIS Act (author interview, Washington, D.C., June 2007; SIRC, 2006, p. 44).

Table 3.1
Median Turnaround Time in Days of CSIS Government Security Screening, 2003–2006

Level	2003–2004	2004–2005	2005–2006
DND Level I (confidential)	20	49	24
DND Level II (secret)	18	63	19
DND Level III (top secret)	96	70	39
Non-DND Level I (confidential)	7	12	15
Non-DND Level II (secret)	11	14	13
Non-DND Level III (top secret)	82	69	60

SOURCE: SIRC, 2006, p. 42.

Table 3.2
Immigration Screening Requests, 2005–2006

Type of Request	Number of Requests[a]	Number of Information or Inadmissibility Briefs
Within and outside Canada	63,200	133
Front-end screening[b]	17,100	89
Refugee determination[c]	11,700	127
Subtotal	92,000	349
Citizenship applications	308,000	120
Total	400,000	469

SOURCE: SIRC, 2006, p. 44.

[a] Figures rounded to the nearest 100.

[b] Represents individuals who arrive at the Canadian border claiming refugee status.

[c] Represents those refugees (as defined by the Immigration and Refugee Protection Act) who apply from within Canada for permanent-resident status.

In the event that a "positive" vet is made, a security certificate is issued; depending on the stance of the government of the day, that certificate can be used to deport the person in question back to his or her country

of origin.[15] Finally, the service evaluates contingency plans for special events and extant site-access programs that protect airports, nuclear-power plants, and facilities subject to parliamentary authority (CSIS, 2005a, p. 13).

As previously noted, CSIS draws on a wide variety of information sources, from HUMINT to SIGINT. These raw data are thoroughly examined by highly qualified, university-educated, career-track threat assessment unit analysts[16] who produce two main types of reports: threat assessments (TAs) and threat and risk assessments (TRAs).[17]

A TA is a short (generally no more than two pages), time-sensitive operational evaluation that aims to alert the central government to terrorist threats that may pose an immediate danger to the country's national stability. For the most part, these reports are written for the security and intelligence communities to enable organizations that must take preventive measures to do so *and* to determine the level of protective resources required.[18] TAs are generated at CSIS' own initiative—and generally whenever threat information or intelligence is received—and disseminated to the service's list of core consumers in the CIC and other federal departments and agencies that might

---

[15] Security certificates are an exceptional measure and can be used to remove only noncitizens who are deemed to pose the greatest threat to Canada and Canadians. Since 1991, 27 such certifications have been issued.

[16] In 2006, CSIS received between 14,000 and 15,000 applications for 100–150 analyst positions, allowing the service to be highly discriminating in its hiring preferences. Typically, only graduates with tertiary-level qualifications will be considered for employment, and all must exhibit, at a minimum, extremely strong research, analytical, interpersonal, and communication (written and oral) skills. CSIS consistently recruits from Canada's leading educational establishments and, in 2007, was nominated by Carleton University as one of its top seven employers of the year (see CSIS, "Notes for Remarks to Carleton University Alumni Association, Rideau Club," May 24, 2007a).

[17] Author interview, Ottawa, November 2003; SIRC, 2006, pp. 39–40.

[18] For example, should a credible threat to the safety of the prime minister surface while he or she was traveling to Toronto, a TA would be used to help determine what sort of accompanying RCMP transit detail would be required and what level of police protection would be necessary once the prime minister arrived.

be interested in the specific threat in question.[19] TAs are thoroughly scrutinized before release and must be strongly substantiated because resulting defensive and preemptive measures can be extremely costly and disruptive (especially if they pertain to aspects of CI).[20]

TRAs, on the other hand, are relatively long-term strategic assessments that, although focused mainly on terrorist issues, incorporate the broad spectrum of functional threat responsibilities that fall to CSIS (i.e., espionage, PMV, counterproliferation, and subversion). Each report is intended to have a shelf life of at least one year (although this varies as circumstances demand) and act somewhat as a reference document. TRAs are produced at the specific request of a federal government department or agency and, once completed, are submitted solely to the requester unless permission for wider dissemination is granted. The assessments are developed from both covert and open-source information, although they typically make considerable use of the latter, especially for the background context (which is more detailed in a TRA than in a TA).[21]

Leadership and Human Capital

Initially, most of CSIS's top leaders were career-track intelligence officers who had previously worked in the RCMP's Security Service and who had risen up through CSIS's ranks. This is no longer the case, however; in the past 5–10 years, CSIS has increasingly emphasized hiring top managers directly from the outside, prioritizing applicants from other government departments (such as DND, Foreign Affairs, and CBSA) or those with extensive senior management experience in the private sector.[22] Like ASIO, CSIS has placed special emphasis on

[19] Under normal circumstances, a TA would not be distributed to the private sector, and it would remain the RCMP's responsibility to disseminate a report to provincial and municipal police.

[20] Author interview, Ottawa, November 2003 (see also CSIS, 2005a, p. 10).

[21] Author interview, Ottawa, November 2003 (see also CSIS, 2005a, p. 10).

[22] Author telephone interview, May 2007.

hiring outsiders for CSIS directorships largely to stifle potentially damaging bureaucratic self-replication and to foster an image of objective leadership "balance." Indeed, since 1984, the post has been filled only once by an individual with an RCMP background: Dale Neufeld held the position for six months during the transition between retired CSIS head Ward Elcock, whose tenure had expired,[23] and the appointment of the current director, James Judd.[24]

Management and Process

As in ASIO, responsibility for management of day-to-day CSIS activities falls to the service's director, who answers to the Inspector General of CSIS and, through him or her, to the PSEP.[25] Meetings with branch heads are held at least once a week to establish work priorities, evaluate progress on specific or ongoing surveillance cases, and determine changing organizational and operational needs. Each division manager is also required to provide an annual report to the director describing activities undertaken during the previous year and the extent to which they accord with the branch in question, the legal CSIS mandate, and overall ministerial direction and propriety. As in ASIO, these branch assessments form the basis of the director's annual report, which details activities down to the tactical level, must be certified by the CSIS Inspector General, and is lodged before the PSEP.[26]

CSIS internal management controls reflect the agency's highly centralized character and are essentially expedited through the following two committees, each of which is chaired by the CSIS director:

---

[23] The CSIS Act specifies that a director can serve only two five-year terms.

[24] Author interview, Washington, D.C., June 2007.

[25] Subsection 6(2) of the CSIS Act authorizes the PSEP to issue written directions to the service's director in the form of a document known as the *National Requirements for Security Intelligence*. This document outlines where the agency should focus its investigative efforts and summarizes its collection, analysis, and advisory priorities (SIRC, 2006, p. 36).

[26] Author telephone interview, May 2007; SIRC, 2006, pp. 31–32. The report to the PSEP is prepared at the top-secret level; an unclassified version of the document is available at CSIS, undated.

- the Target and Approval and Review Committee (TARC), which decides whether a particular group or individual should be subject to CSIS investigation and, if so, what level of intrusiveness is appropriate under the particular circumstances.[27] Acting through TARC, the service's senior management is thus able to launch internal inquiries into the agency's operations and determine the specific scope and dimensions such inquiries should take.[28]
- the Security Intelligence Review Committee (SIRC),[29] which adjudicates all warrant applications submitted to the federal court under Section 21 of the CSIS Act. In this instance, working through the SIRC allows CSIS's senior management to independently examine the agency's most intrusive investigative powers and ensure that they are appropriate for and proportionate to the purpose for which they are requested.[30]

Organizational Structure and Funding Patterns

Reflecting CSIS's shift in perspective in response to the transnational and international nature of current threats, in May 2006, CSIS modified its original, issue-oriented structure[31] to one that is now defined largely along geographic lines delineated in the following manner:

- an International Terrorism which deals with Sunni and Shi'a extremism in Canada and overseas

---

[27] Section 20 of the CSIS Act requires that all cases in which service employees may not have complied with legislation or policy or may have acted unlawfully in the performance of their duties, be reported and investigated. This provision helps ensure that unlawful activities not detected by provincial law enforcement agencies will still be reported to the minister.

[28] Author interview, Washington, D.C., June 2007.

[29] The SIRC does not act as a fully internalized control mechanism, as it includes legal representation from both the Department of Justice and Public Safety Canada.

[30] CSIS, 2005a, p. 18; author interview, Washington, D.C., June 2007.

[31] Historically, CSIS was divided into three main divisions that were defined in strict functional terms: CT, counterintelligence (which included mitigation of espionage and foreign-influenced activities), and counterproliferation (with the focus on weapons of mass destruction).

- a Middle Eastern and Africa division, which focuses primarily on weapons of mass destruction proliferation concerns, groups and movements associated with the global jihadist network, and rogue regimes (such as Iran)
- an Asia, Europe, and Americas division, which addresses domestic extremism in Canada (the main emphasis being on right-wing and neo-Nazi militancy), non-Islamic militant groups of concern (e.g., LTTE), and Russian and Chinese activities aimed at "stealing" Canadian-patented or Canadian-sourced technology.[32]

In pursuing these various tasks and functions, CSIS employs 2,423 people (as of 2007)[33] and, at the time of this writing, ran on an operational budget of C$3.45 billion (CSIS, 2005a, pp. 25–26). The service plans to further expand its human-resource base during the next several years; it will also receive an anticipated increase to its operating budget of at least C$500 million between fiscal years 2008 and 2012.[34]

Key Relationships with Other Intelligence and Law Enforcement Agencies

The Canadian Intelligence Community

CSIS interaction with the wider CIC is carried out primarily through the ITAC, which is housed in CSIS's headquarters in Ottawa and is designed to act as a clearinghouse for assembling, integrating, analyzing, and sharing intelligence provided by a wide range of sources. The center works closely with the National Security Advisor to the Prime Minister (who appoints the ITAC director) and includes representatives from relevant federal and provincial security organizations.[35] In addition, the center has established liaison agreements with counter-

[32] Author interview, Washington, D.C., June 2007.

[33] Compare this figure to a pre-2001 staffing level of 2,097 personnel.

[34] Author interview, Washington, D.C., June 2007.

[35] At the time of this writing, CSIS had 29 memoranda of understanding with domestic partners to avail the exchange of information and "single voice" interagency ITAC assess-

part organizations in the UK, the United States, Australia, and New Zealand (CSIS, 2005a, pp. 14–15).

CSIS also acts as a central partner agency in the Integrated National Security Enforcement Teams, which were established in 2002 in Vancouver, Montreal, Toronto, and Ottawa.[36] These multipronged task forces are made up of officers seconded from CSIS, the RCMP, CBSA, Citizenship and Immigration Canada, and police forces drawn from the provincial and municipal levels. They are designed primarily to (1) help increase the country's overall capacity to collect, share among partners, and analyze intelligence on targets that threaten national security and their related criminal activities and (2) create an enhanced enforcement capacity to bring such targets to justice (CSIS, 2005a, pp. 15–16).

Law Enforcement

Prior to 9/11, CSIS links with law enforcement were defined essentially in terms of a bilateral working partnership with the RCMP. Like the AFP, its counterpart in Australia, the RCMP is responsible for overseeing all matters that pertain to national (as opposed to provincial/territorial) policing in Canada. Furthermore, under the provisions of the 2001 Anti-Terrorism Act, the RCMP assumed a principal role for combating any PMV that is relevant to the country's internal security.[37] CSIS ties to the RCMP evolved steadily, moving out of a period of initial antipathy following the creation of CSIS in 1984 (which robbed the RCMP of its domestic security intelligence function) into a current

---

ments. Of these 29 memoranda, 17 were agreed to by federal agencies or departments and 10 by provincial and municipal entities (SIRC, 2006, p. 35).

[36] Author interview, Washington D.C., June 2007.

[37] SIRC, 2006, p. 40. It should be noted that, since 9/11, provincial and municipal police forces have assumed greater responsibility for investigating terrorism-related cases. This is because of the limited resources available to the RCMP and the fact that, in most instances, problems of PMV originate in large metropolitan centers whose extensive racial diversity and multicultural character make it more logical for municipal and provincial forces to take the lead. That said, because most provinces contract their policing function to the federal government (the two exceptions being Ontario and Quebec), the RCMP, by default, continues to assume primary responsibility for investigating most terrorism-related crime (author interview, Ottawa, November 2002; see also Austen, 2007a).

relationship based on mutual respect and trust.[38] At the heart of this relationship is a well-established secondment and liaison arrangement instituted on both an ad hoc basis and a permanent one.[39] CSIS-RCMP interaction is a central feature of ITAC and the Integrated National Security Enforcement Teams previously discussed and is strengthened by the organizations' joint participation in the National Counter-Terrorism Plan, which serves as the main coordinating mechanism for streamlining Canadian responses to terrorist threats and incidents that take place in Canada (CSIS, 2007b, p. 10).

In 2007, there was speculation that CSIS might start to engage in more evidentiary-standard intelligence collection and assessment in the future in order to avail closer information collaboration with the RCMP. However, it seems that this is unlikely to occur because many in CSIS fear that it would not only compromise the identity of covert human sources but could also fundamentally alter the nature and purpose of the agency's work. As one official remarked to the author,

> CSIS does not interpret the end game of counterterrorism in the minutiae of individual arrests and prosecutions; by contrast, the service views its role in far broader, strategic terms, which are essentially aimed at securing Canada's long-term security interests and safeguarding the welfare of its citizens.[40]

CSIS also places considerable emphasis on working closely with provincial and municipal police forces, not least because it is in multicultural and racially diverse cities such as Vancouver, Montreal, and Toronto that most problems of PMV originate. To expedite contact and the flow of information between these agencies, CSIS runs several regional suboffices and associated outreach initiatives that are formu-

---

[38] To a large extent, this has been availed by written protocols that clearly spell out what CSIS and the RCMP can and cannot do in terms of interagency operations and information exchange.

[39] Author interview, Washington, D.C., June 2007. Agreements between CSIS and the RCMP allow for the mutual exchange of personnel; at any one time, there will be at least one officer from each agency permanently assigned in a senior liaison capacity.

[40] Author interview, Washington, D.C., June 2007.

lated specifically to facilitate two-way data exchanges that ensure that threat assessments are up to date and accurate and helps speed the process through which classified material is translated into actionable intelligence on the ground.

Oversight

A rigorous system of external oversight and accountability accompanies the intelligence setup in Canada. Indeed, more than two-thirds of the CSIS Act is devoted to describing how the service's activities are to be monitored, evaluated, and approved by third parties not formally associated with the service's day-to-day operations. The degree of accountability demanded of CSIS sets the service apart from many similar agencies around the world and has been used as a model for informing the development of newly configured domestic security institutions in countries emerging from highly authoritarian and nondemocratic rule (such as the Republic of South Africa).[41]

The CSIS Act establishes two main external oversight entities for the agency—SIRC and the CSIS Inspector General—both of which are responsible to the PSEP, who is answerable to Parliament for the service as a whole.[42]

SIRC acts as an independent review agency and is staffed by three to five privy councilors[43] who are appointed by the governor in council after consultation with the prime minister and leaders of the opposition parties. Through the PSEP, SIRC reports to the legislature. SIRC is

[41] Author interview, Ottawa, December 2002 (see also CSIS, 2005a, p. 17).

[42] Besides these formal structures, other bodies—including the Auditor General, the Information Commissioner, the Privacy Commissioner, and various royal commissions—have periodically carried out external scrutiny of CSIS activities.

[43] At the time of this writing, SIRC consisted of the Honorable Gary Filmon (the committee chairman), the Honorable Raymond Speaker, the Honorable Baljit Chadha, the Honorable Roy Romanow, and the Honorable Aldea Landry. These members were supported by an executive director (Susan Pollak) and a staff of 19: an associate executive director, senior counsel, a senior adviser, a corporate services manager, counsel, a senior paralegal (who also serves as the Access to Information and Privacy Officer), four administrative staff, and nine researchers (SIRC, 2007, p. 54).

the only independent body equipped with the legal mandate to review CSIS activities. The CSIS Inspector General is authorized to monitor and certify CSIS's compliance with its operational policies and to certify the extent to which he or she is satisfied with the agency's internal corporate management procedures. The CSIS Inspector General functions as the "eyes and ears" of the PSEP, validating CSIS's activities and ensuring that they conform with the CSIS Act and overall ministerial direction (CSIS, 2004, p. 2; SIRC, 2006, pp. 3, 32).

SIRC and the CSIS Inspector General exercise their oversight functions in a largely similar manner. They are empowered to open inquiries at their own behest or in response to outside requests and they have a virtually unrestricted ability to investigate complaints made against serving CSIS officers[44] and audit the service's policy, administration, and finance. (Note, however, that SIRC is precluded from purveying cabinet confidences or material that either relates to active operations or could expose the identity of a confidential intelligence source). In more-specific terms, these duties may involve one or more of the following activities (see R.S.C. 1985, c. C-23, Chapters III.29 and III.38):

- generally reviewing CSIS's performance of its duties and functions
- arranging for additional reviews to be conducted pursuant to relevant clauses of the CSIS Act
- investigating complaints made against CSIS or its case officers[45]
- monitoring, reviewing, and certifying CSIS operational policies.

---

[44] New guidelines were introduced in January 2006 to streamline SIRC complaint hearings, most of which are aimed at resolving preliminary procedural matters, such as the allegations to be investigated and the identity and number of witnesses to be called. Provided that no issues of national security are raised, these matters can be undertaken by telephone, and a transcript is provided to relevant parties at a later date.

[45] Before SIRC investigates a complaint, two conditions must be met. First, the complainant must have lodged a written submission to the CSIS director and not received a response that was both timely (generally defined as within 30 days) or satisfactory. Second, the complaint itself must not be trivial, frivolous, or vexatious or be made in bad faith. In general, four main kinds of issues may be investigated by SIRC: (1) those lodged by persons "with respect to any act or thing done by the Service" (Section 41 of the CSIS Act), (2) those concerning denials of security clearances to government employees or contractors (Section 42 of the CSIS Act), (3) those referred by the Canadian Human Rights Commission, and (4) those contained in PSEP reports and made in relation to the Citizenship Act.

The Federal Court of Canada also exercises important judicial control over CSIS and, as in Australia, is the only entity that can authorize a warrant allowing the institution of special powers. Obtaining approval is the product of an intensive decisionmaking process consisting of several steps. First, CSIS issues an affidavit that justifies the need for the specific measure in question. Then, SIRC reviews this submission to assess its overall validity. If the committee decides to proceed with the warrant application, the request is forwarded to the PSEP for his or her consideration. Only after the application receives the minister's approval is a presiding judge of the Federal Court brought in to issue a final decision on the action's necessity and appropriateness (CSIS, 2004, p. 47; *Terrorism: Special Investigation Techniques*, 2005, p. 481). As in Australia, there is no such thing as an "omnibus" warrant that sanctions a bundle of intrusive investigation techniques: All requests are reviewed and assessed individually.

Special powers can be authorized for both reactive and proactive investigations, the former essentially remaining the remit of law enforcement, the latter of the intelligence community. When employed specifically for CT purposes, provisions governing these methods allow for somewhat greater latitude than exists in "more-conventional" criminal investigations. For example, warrants pertaining to communication intercepts normally expire after 60 days; however, in the case of potential terrorism offenses, they can be authorized for a full year. In addition, unlike more-general investigations, there is no requirement to demonstrate that other forms of (less intrusive) surveillance have been tried and failed, are unlikely to succeed, or are impractical given the urgency of the matter (*Terrorism: Special Investigation Techniques*, 2005, p. 483).

At the completion of a complaint hearing, SIRC prepares a report outlining its findings and any recommendations the committee members consider appropriate. This is then sent to the PSEP, the director of CSIS, and the complainant. However, any information that has national security implications is not included (see SIRC, 2006, pp. 19–20).

Performance Metrics

Unlike ASIO, CSIS does not rely heavily on surveys of customers to determine satisfaction with the agency's products. As one former senior officer remarked, "the Service does not attach too much importance to these types of qualitative judgments, largely because questionnaires are either only partially answered or not returned at all."[46] Far more stock is placed in the periodic reviews of CSIS's performance that are undertaken as a routine function of SIRC and the CSIS Inspector General. In essence, both bodies perform this duty by identifying and evaluating completed and ongoing projects from the previous year and providing a retrospective assessment of specific CSIS activities and investigations (CSIS, 2005a, p. 17). In its 2005–2006 operational review of CSIS, SIRC concluded that, after 21 years, CSIS continued to work well and had demonstrated both a willingness and a capacity to adapt and adjust to the demands of a rapidly changing global environment (SIRC, 2004).

CSIS has also developed, or is in the process of developing, internal mechanisms for gauging its output. In 2006, the service established a small unit to develop specific performance standards for formally grading CSIS reports and assessments; it is now standard practice for all products to be measured against these metrics.[47]

To track the efficiency of its security screening, CSIS calculates the median number of days it takes to process requests for clearances.[48] As noted in Table 3.1, between 2005 and 2006, turnaround times for DND ranged from 24 days for Level I clearances to 39 days for Level III clearances. These figures represent a significant improvement over the 2004–2005 reporting period, whose turnaround times in days were 49 and 70, respectively (SIRC, 2006, p. 42).

---

[46] Author telephone interview, May 2007. Of the various surveys that are undertaken, it is feedback from DND that is taken most seriously. This reflects the fact that Defense is the Service's most important customer.

[47] Author interview, Washington, D.C., June 2007.

[48] CSIS records its turnaround statistics in median rather than average numbers to mitigate the impact of unusually short or lengthy processing times; this provides a more accurate measure of how quickly a typical security assessment is prepared.

Finally, there are plans to introduce new procedures for determining the overall "worth" of specific programs by evaluating their individual benefit in terms of per-unit dollars spent. According to one official, this remains a personal priority of the director and is an initiative aimed primarily at ensuring that the projected influx of C$500 million in operating funds through 2012 is spent in the most cost-effective manner possible.[49]

Problems or Controversies

CSIS has been largely free of major periods of crisis and abuse. A few notable incidents, however, have generated some concern about the service's overall operational effectiveness and control. In 1985, the thoroughness of CSIS covert surveillance was questioned following a siege on the Turkish embassy that resulted in one fatality (a security guard) and 12 abductions and left the ambassador, Coskun Kirca, with serious injuries.[50] The attack stoked debate primarily because it was claimed by right-wing paramilitaries—in this instance, operating under the banner of the Armenian Revolutionary Army—that had already been implicated in two prior strikes on senior diplomatic officials stationed at Ankara's mission in Ottawa.[51]

That same year, a midair explosion destroyed a Boeing 747 en route from Canada to Delhi, killing all 329 on board.[52] The attack, which was attributed to Sikh extremists based in British Columbia, led to an official board of inquiry whose final report (issued in 2007) heavily faulted CSIS for failing to adequately act on information pro-

[49] Author interview, Washington, D.C., June 2007.

[50] Petter, 2005. The ambassador sustained several broken bones after jumping from a second-story window to escape the assailants.

[51] In 1982, Kani Gungor, the embassy's commercial attaché, was permanently paralyzed after being shot in the parking garage of his residence. Several months later, Colonel Atilla Altikat, Turkey's military attaché to Canada, was assassinated while driving to work. Both attacks were attributed to Armenian paramilitary groups (author interview, Washington, D.C., June 2007).

[52] Prior to 9/11, this was the most destructive act of aviation sabotage in history.

vided by a Vancouver police officer—information that suggested that a violent incident was being planned.[53] The inquiry also heavily criticized the RCMP for its failure to share with the intelligence service a specific warning that it had received from the Indian government (and Air India itself) three weeks prior to the bombing.[54]

In 1994, the service became embroiled in what was to become known as the Heritage Front affair. The incident revolved around the activities of Grant Bristow, a CSIS mole who was recruited to gather intelligence on xenophobic, neo-Nazi organizations operating in Canada. Bristow subsequently became one of the main leaders of the Heritage Front, a radical white-supremacist movement that was implicated in various harassment campaigns (some of which were violent) against antiracist protesters and Jewish community leaders and representatives.[55] Bristow himself was accused of being complicit in Heritage Front funding and recruitment efforts; instrumental in advising the far right on security and counterintelligence; and active in spying on the Canadian Broadcasting Corporation, the Canadian Union of Postal Workers, and the Reform Party—all with CSIS's explicit knowledge and approval. While a SIRC investigation ultimately exonerated the service and Bristow of any major transgressions,[56] it did conclude that the overall level of policy guidance available to CSIS officers for handling inside intelligence assets was seriously deficient.[57]

---

[53] According to the testimony of the (now former) officer, Don McLean, an oral exchange captured on tape between two Sikhs who were under surveillance in an unrelated criminal investigation heavily implied that some violent incident would occur within two weeks. Although McLean passed details of the conversation to CSIS, the information was filed away as "unconfirmed." See "Police Had Hint," 2007.

[54] "Canadian Agencies Were Warned," 2007; "Police Had Hint," 2007. For an in-depth account of the attack, see Jiwa, 1987.

[55] Author interview, Washington, D.C., June 2007.

[56] The SIRC inquiry specifically noted that "active" sources were necessary to provide high-grade intelligence to the security services, and that information provided by Bristow contributed to 80 TAs over five years, hundreds of reports, and the deportation of at least five foreign white supremacists.

[57] SIRC raised a number of important questions and issues, including the following: *What kind of proactive role is acceptable for a source in an organization targeted by CSIS? Is it appropri-*

Most recently, CSIS was criticized for failing to take adequate action to secure the speedy release of Maher Arar, a Canadian citizen who was seized and secretly transported to Syria (the country of his birth) by U.S. authorities while transiting John F. Kennedy International Airport in 2002. Arar was imprisoned in a Damascus military intelligence facility for nearly a year, during which time he was interrogated, tortured, and subjected to degrading and generally inhumane conditions. He has never been charged with any offense in Canada, the United States, or Syria, and there is no evidence that he ever constituted a threat to Canadian national security. An official commission of inquiry established to examine the scandal published its findings in 2006. Although much of the focus of the commission's inquiry was the RCMP and the nature of the ultimately false and inflammatory claims that the force made against Arar,[58] the commission did take issue with CSIS on two counts (see Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, 2006, p. 15):

- failing to (1) perform an adequate reliability assessment on the veracity of self-incriminating statements procured from Arar while in Syrian custody and (2) determine whether these were coerced through torture
- failing, once it became clear that Arar represented no threat to Canadian national security, to explicitly alert relevant U.S. and Syrian authorities of that fact.

---

ate for a source to direct or lead an organization or movement? Should sources be engaged in countermeasures that would serve to destroy (rather than maintain) terrorist groups or movements? Do the benefits of maintaining a source outweigh the benefits to be gained from taking measures (i.e., with the police) to destroy the group? For a full account of the investigation, see SIRC, 1994.

[58] The RCMP investigation into Arar was conducted through Project A-O Canada. The unit was created in the aftermath of 9/11 and directed to carry out surveillance, centered in Ottawa, on individuals associated with al Qaeda and suspected of planning terrorist attacks in North America. The commission concluded that Project A-O Canada "provided American authorities with information about Mr Arar that was inaccurate, portrayed him in an unfairly negative fashion and over-stated his importance [to] RCMP [CT] investigations." Following the report's release, the force's commissioner, Giuliano Zaccardelli, resigned (see Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, 2006, p. 13; Austen, 2007a, 2007b).

Conclusion

In many ways, the CSIS case mirrors the ASIO example. The service's functional role has grown in tandem with the altered threat environment brought about by al Qaeda's 9/11 attacks and is currently executed by a staff of 2,423 with an operating budget of nearly C$3.5 billion. Like its Australian counterpart, CSIS has no independent power of arrest; is subject to rigorous and routine executive, legislative, and judicial oversight; and enjoys established coordination and liaison arrangements with the police and other agencies (such as customs and immigration and the coast guard) with a mandated role in homeland security.

CSIS is unique, however, in the sense that it was deliberately created to separate law enforcement agencies (i.e., the RCMP) from intelligence activities. The service's early experience demonstrates the type of interagency hostilities that can arise under such circumstances and the negative implications these can have for national security. In addition, CSIS has always had both an internal and external focus, reflecting the fact that Canada does not have a dedicated foreign intelligence bureau per se and that many of its domestic threats are rooted in conflicts outside Ottawa's sovereign borders. Hence, despite its relative "youth" compared to other intelligence agencies—such as ASIO, the UK's Security Service (better known as MI5), and France's Direction de la Surveillance du Territoire, CSIS has been equally (if not more) adept in adjusting to the requirements of a modern-day terrorism challenge that has increasingly blurred erstwhile distinctions between the domestic and international realms.

CHAPTER FOUR

France

Richard Warnes

Of all the European countries, France may have the most experience in using intelligence to counter both insurgency and terrorism. As of this writing, the principal domestic intelligence organization in France is the Direction de la Surveillance du Territoire [Directorate of Territorial Surveillance] (DST),[1] but there is also the Direction Centrale des Renseignements Généraux [Central Directorate of General Intelligence] (DCRG); both organizations are controlled by the Police Nationale. Under the overarching direction of the Ministère de l'Intérieur, the DST is equivalent to the UK's MI5; the DCRG is equivalent to the UK Special Branch, a police intelligence organization. We focus primarily on the DST, but because the DST and the DCRG are currently being amalgamated into a single domestic intelligence organization, we also examine certain aspects of the DCRG's history, structure, and mission.[2]

Creation and Relevant History

The DST emerged from the wartime Free French intelligence organization, the Bureau Central de Renseignements et d'Action [Central

[1] During the course of 2008, the DST and DCRG were merged to form a new organization, known as the Direction Centrale du Renseignement Interieur [Central Directorate of Interior Intelligence] (DCRI). When writing about the history and structure of France's principal domestic intelligence organization, however, we use DST.

[2] This chapter was written at the end of 2007.

Office of Intelligence and Operations] (BCRA), following an order of November 16, 1944, signed by General Charles de Gaulle. As a domestic intelligence and internal security organization, the DST inherited the title of the prewar Surveillance du Territoire [Territorial Surveillance] and was placed under the administrative control of the Ministère de l'Interieur. The DCRG had older roots, based in the Third Republic, as, in 1911, the original Brigade des Renseignements Généraux [General Intelligence Brigade] was formed by Célestin Hennion, the director of la Sûreté [Safety or Security], the criminal-investigation unit of the Police Nationale [National Police]. The current DCRG reemerged in 1937 with the formation of the Direction des Services de Renseignements Généraux et de la Police Administrative [Directorate of General Intelligence and Police Administrative Services] (see Ministère de l'Interieur, 2006). Thus, unlike the DST, which emerged after liberation and from within Gaullist Free French circles, the DCRG was closely associated with service at the behest of the Vichy regime, particularly the rounding up of Jews, communists, and Resistance members. This different heritage resulted in differences in postwar attitudes, ethos, and cultures between the two organizations.[3]

Led by Roger Warin (aka Wybot), the former wartime head of the counterespionage section of the BCRA, the DST's initial role was to identify and detain former collaborators and agents of the Axis powers (see Thuillier, 2000). However, "the rivalry between the DST and the [DC]RG to corner the market in the prosecution of collaborators became so intense that [DC]RG director Marc Berge publicly denounced Wybot for stonewalling [DC]RG investigations" (Porch, 1997, p. 269). Both organizations also countered the "threat to the democratic system" posed by the power of the Parti Communiste Français [French Communist Party] (PCF) and its control of the trade-union movement (especially of the Confédération Générale du Travail [General Confederation of Workers]—one of the largest and most active of the French trade unions, closely associated with the PCF) (see Beevor and Cooper, 2004). However, these tasks proved troublesome—the first because of changing allegiances, the level of wartime collabora-

[3] Author interview with a senior French intelligence official, October 2007.

tion, the role of the previous Vichy regime, and the destruction of wartime records (which made it difficult to identify, quantify, and corroborate many people's actions during the war); the second because the PCF, which had a wartime record of resistance, claimed one-quarter of the popular vote at the time and, until 1947, sat in the French government (see Porch, 1997).

From 1946 onward, although there were a growing number of attacks by the Viet Minh against the French authorities in France's Indo-Chinese colony of Vietnam,[4] the recently formed DST played only a limited role in monitoring activists from the Vietnamese community in mainland France. Its main focus was on counterespionage—in particular, the Cold War threat to French security posed by the actions of the Soviet Komityet Gosudarstvennoy Bezopasnosty [Committee for State Security] (KGB) (see Faligot, 2006c). Indeed, "for much, probably most, of the Cold War, the Paris residency ran more agents—usually about 50—than any other KGB station in Western Europe" (Andrew and Mitrokhin, 2001, p. 460). At the same time, the vast majority of intelligence activity to counter the Viet Minh necessarily occurred within Vietnam and Indo-China and was coordinated by the recently formed postwar successor to the BCRA, the Service de Documentation Extérieure et de Contre-Espionnage [Service for External Information and Counterespionage], and by French military intelligence (see Porch, 1997, Chapter 12). Following a series of French defeats culminating in the loss of the battle of Dien Bien Phu in 1954 (see Windrow, 2004; Fall, 1985), in which the failure of military intelligence played a significant role (see Le Page, 2007), the French authorities withdrew from Vietnam. However, both the DST and the DCRG were destined to play a far more active role in the nationalist insurgency that was emerging from within French territory overseas: Algeria.

Due to Algeria's status as an integral part of Metropolitan France and the fact that Algeria hosted more than 1 million French and other Mediterranean *Pieds-Noirs* ["Black-Feet," or colonists], the DST was directly involved in countering the nationalist insurgency that was developing there in the 1950s. The DST had already presented

[4] For more details about the conflict, see Fall, 2005.

a detailed report of the growing threat prior to the initial November 1, 1954, bomb attacks in Algiers and other major cities but for political reasons, the French authorities had failed to heed these warnings. Subsequently, as well as operating in Algeria proper, the DST became active in mainland France, where elements within the sizable Algerian minority community and members of the PCF provided both active support and funds to the Front de Libération Nationale [National Liberation Front)] (FLN) campaign and where a number of foreign diplomats, particularly Egyptians and Cubans, were actively supporting the insurgency (see Porch, 1997).

Following the "Generals' putsch" of April 1961 (see Porch, 1993, Chapter 29) and de Gaulle's 1962 decision to grant Algeria independence, it was the DCRG (not the DST) that was tasked with countering the threat posed by the Organisation de l'Armée Secrète [Organization of the Secret Army] (OAS), an organization of disgruntled military veterans from Algeria and *Pieds-Noirs* who felt betrayed by de Gaulle's decision (see Dard, 2007; Kauffer, 2006c, pp. 94–100). This was because many of the DST officials involved in the Algerian conflict were themselves *Pieds-Noirs*, leading to concerns about their loyalty; hence, it was easier and more reliable to use the DCRG.[5] Ultimately, this decision led to the creation within the DCRG of a new section to monitor *mouvements révolutionnaires* [revolutionary movements]. Nevertheless, there remained mixed loyalties among many military, intelligence, and police officials, and the resulting seriousness of this threat was highlighted by an OAS campaign of bombings and assassinations (see Parker, 1998, Chapter 17), including the nearly successful attempt to kill President de Gaulle at Petit-Clamart on August 22, 1962.[6] Ultimately, the OAS leadership were decimated by arrests, imprisonments, the French authorities' use of deniable *barbouzes*[7] teams against them,

[5] Author interview a with senior French intelligence official, October 2007.

[6] In total, more than 30 attempts were made on de Gaulle's life.

[7] Semicriminal elements whom the authorities used to counter the OAS by direct action (see Kauffer, 2006c, pp. 65–75).

and several executions;[8] these events led ultimately to the organization's dispersal.

In the field of counterespionage, the DST and the DCRG were extremely active in countering the activities of Soviet agents and their French sources during the Cold War. The DCRG focused its surveillance expertise on PCF members involved in subversion and espionage (see Gomart, 2007), while the DST was instrumental in the recruitment of KGB officer Vladimir Vetrov (aka Farewell), who supplied nearly 4,000 classified documents to the French external intelligence service, the Direction Générale de la Sécurité Extérieure [General Directorate for External Security] (DGSE) before his arrest and execution by the Soviet authorities in 1982 (see Merlen and Ploquin, 2003). However, such successes were tempered by allegations, such as those of a Soviet defector code-named Martel, that the French intelligence services and diplomatic corps were infiltrated by Soviet agents at the highest levels (see Porch, 1997).

The DST's role in countering international terrorism inspired from abroad first came to public attention in 1975, when two of its officers, Inspectors Raymond Doubs and Jean Donatini of Division B2 (a division formed that year and responsible for international terrorism inquiries), were shot dead after confronting the noted international terrorist "Carlos" (see Violet, 1996) in an apartment in the rue Toullier in Paris (see Dobson and Payne, 1977). The DST later played a key role in identifying and stopping an Armenian Secret Army for the Liberation of Armenia (ASALA) cell after ASALA murdered two people at the Turkish embassy in Paris in March 1981, took staff hostage at the Turkish consulate in Paris in September 1981, and bombed the Paris-Orly Airport in 1983. The DST was also central to investigations of a wave of bombings in 1986 (see Shapiro and Suzan, 2003, p. 72) that culminated in the deaths of six people in an explosion on the rue de Rennes in Paris on September 17, 1986. At first, these attacks were believed to be linked to a group of Arab terrorists associated with the Comité de Solidarité avec les Prisonniers Politiques Arabes et du

[8] In particular, those of Lieutenant Colonel Jean Bastien-Thiry, Lieutenant Roger Degueldre, and Sergeant Bobby Dovecar.

Proche-Orient [Solidarity Committee with Arab Political Prisoners and the Middle East]. However, a DST informant provided crucial information that highlighted the Iranian backing for the terrorist cell that was targeting France because of the country's decisions to supply arms to Iraq during the first Gulf War and become involved in Lebanon (see Porch, 1997).

Meanwhile, due to its mandate to counter terrorism of domestic origin, the DCRG was tasked with countering the various forms of nationalist terrorism posed by (1) extremist Corsicans of the various factions of the Front de Libération Nationale de la Corse [Corsican National Liberation Front] and associated groups (see Farrugia and Serf, 2004; Follorou and Nouzille, 2004), (2) the Front de Libération de la Bretagne [Brittany Liberation Front], (3) the Armée Révolutionnaire Bretonne [Breton Revolutionary Army] (see Baud, 2003; Parmentier, 2006), and (4) the Basque Euzkadi Ta Azkatasuna [Basque Fatherland and Freedom] and Iparretarrak extremists in France (see Cettina, 2003). The DCRG, with the support of Police Judiciare [Judicial Police] detectives, was also actively engaged in countering the political terrorism of the extreme-left-wing Action Directe [Direct Action] (AD) in the 1980s (see Dartnell, 1995; Hamon and Marchand, 1986). Led by Jean-Marc Rouillan, Nathalie Ménigon, Georges Cipriani, Joëlle Aubron, and Régis Schleicher, AD was responsible for a wave of attacks against official government buildings, including the March 15, 1980, bombing of the DST building. The group was also involved in a number of shootings, including the murders of police and security guards during armed "fund-raising" robberies and the murder of DCRG informant Gabriel Chahine by Schleicher in March 1982. The AD's highest-profile attacks were the January 25, 1985, assassination of General René Audran, director of international affairs at the Ministère de la Défense [Ministry of Defense], and the November 17, 1986, assassination of Renault chair George Besse (see Action Directe, 1992; Villatoux, 2007). However, this spree of attacks ended when the French police organization named RAID (Recherche, Assistance, Intervention, Dissuasion [Research, Assistance, Intervention, Dissuasion]) arrested four of the remaining group leaders at a farmhouse in Vitry aux Loges in Loiret in February 1987; Schleicher had already

been arrested (see Courtois, 1999; Direction Générale de la Police Nationale, 2005).

The DST and DCRG were again prominently involved in a CT role when France's support of the Algerian military government (see Faligot, 2006b) led Islamist extremists linked to GIA to attack French nationals in Algeria, kill three gendarmes and two diplomats in Algiers in August 1994 (see Bétry, 2001, pp. 52–61), and launch a series of attacks in mainland France (see Stora, 2001). These attacks consisted of a December 1994 aircraft hijacking (see "Le Cauchemar de l'Airbus Alger-Paris," 1995; "La Mission," 1994), a series of bomb attacks in the summer and autumn of 1995 (see Shapiro and Suzan, 2003, p. 81), and the final bombing of a *Réseau Express Régional* [Regional Express Network] (RER) rail line in December 1996.[9] The Air France hijacking was brought to a conclusion by the tactical intervention of the Groupe d'Intervention de la Gendarmerie Nationale [Intervention Group of the National Gendarmerie] (GIGN) at Marignane Airport in Marseille (see Bernard, 2003; Harclerode, 2000, Chapter 12; Micheletti, 1997). However, the four terrorists who seized the aircraft had planned to crash it in or blow it up over the heart of Paris.[10] The bombs on the Paris metro and in public areas the following year and at the end of 1996 killed 10, wounded scores (see Kepel, 2003, Chapter 11), and led to DST and DCRG involvement in identifying the GIA-associated groups behind these bombings. Khalid Kelkal's group in Vaux-en-Velin and cells in Chasse-sur-Rhône and Lille (see Cettina, 2003) were dismantled within months of the initial bombings. The investigation culminated in Kelkal's death in a shootout with gendarmes of the Escadron Parachutiste d'Intervention de la Gendarmerie Nationale [Parachute Intervention Squadron of the National Gendarmerie] at Maison Blanche in the region of Lyon on September 29, 1995 (see Bétry, 2001, p. 59).

The current primary focus of both the DST and the DCRG is the threat posed to France and French interests through conspiracies planned by cells linked to or associated with the al Qaeda network (see

[9] For a detailed list of the GIA attacks, see Cettina, 2003.

[10] Author interview with a former intelligence official, July 2005.

Premier Ministre, 2006, Appendix 2). These threats have included the 1998 conspiracy involving Nizar ben Abdelaziz Trabelsi (an al Qaeda terrorist) to attack the FIFA World Cup, the arrest of a Frankfurt cell in 2000 before its attack on the Strasbourg Christmas market, the breakup of the Djamel Begal network in September 2001 before an attack on the U.S. embassy in Paris, and the breakup of an Algerian cell in Saint-Denis that was targeting a Franco-Algerian football match in October 2001. More recently, the French intelligence and policing organizations have been involved in the apprehension of cells in La Courneuve and Romainville linked to the Benchellali family, which through its Chechen contacts was planning an unconventional attack on the Russian embassy in Paris in December 2002. The organizations were also involved in the June 2003 arrest of Karim Mehdi, who was planning attacks on tourist sites in Réunion. In September 2005, the authorities launched an operation against a cell of former GIA members, including M'Hamed Benyamina, who were planning attacks on the DST headquarters, the Paris metro, and Paris-Orly Airport. The DST was actively involved in disrupting French nationals' plans to take part in jihad in Iraq in 2004 and 2005.[11] Despite its focus on this type of threat, however, the DST is still also responsible for counterespionage in France and for protecting classified economic and scientific material and facilities (see Chalk and Rosenau, 2004).

Of particular concern to the DST and the DCRG is the Groupe Salafiste pour la Prédication et le Combat [Salafist Group for Prayer and Combat] (GSPC) (see Schanzer, 2004), which emerged as a radical offshoot of the GIA following the Algerian Civil War of the 1990s. The organization combines a historical anticolonial hatred of France with an affiliation with the al Qaeda network; in fact, it recently renamed itself Al-Qaida pour le Maghreb Islamique [al Qaeda for the Islamic Maghreb] (AQMI). Osama bin Laden's deputy, Ayman al-Zawahiri, has asked the organization to be a "thorn in the throat of France," and AQMI's impact can be seen both in the introduction of suicide car-bomb attacks in Algeria (such as the one against an Algerian government headquarters building on April 11, 2007) and in the deliber-

[11] For more details, see Rodier, 2006.

ate targeting of foreign nationals (such as attacks on U.S. and Russian nationals and the September 21, 2007, wounding of two French citizens).[12] The threat posed by AQMI is of particular concern to the DST and the DCRG due to the large size of France's predominantly Algerian and North African Muslim minority population (which numbers an estimated 5 million or more)[13] and to growing concerns about radicalization amongst its alienated youth in the *banlieue* [suburbs, often poor] of Paris[14] and other major French cities, such as Lyon and Marseilles.

Mission and Critical Capabilities

The DST's missions are outlined under Articles 1 and 2 of the *Décret n° 82-1100 du 22 décembre 1982* and the organization is currently mandated to research and prevent, on the territory of the French Republic, activities inspired, committed or sustained by foreign powers, and constituting a threat to the security of the country. This differs significantly from the broader mandate of the DCRG, which is contained in the *Décret n° 95-44 du 16 janvier 1995*, Article 3:

> [Conduct] the research and centralization of intelligence destined to inform the Government; [the DCRG] will participate in the defence of the fundamental interests of the state; it will combine the general mission of interior security.

This broader mandate means that although the collection of information relating to terrorism may be one of its current priorities, the DCRG also gathers intelligence on a range of political and social issues, thereby allowing the government and senior officials to gauge the general public feeling and "temperature" of the country on a range of sub-

---

[12] Author interview with a senior French intelligence official, October 2007.

[13] Due to France's policy of *laïcité* [laicity or secularism], French authorities do not keep exact figures based on religious beliefs.

[14] Such as Créteil, Argenteuil, La Courneuve, Bobigny, and Montreuil.

jects.[15] In addition to informing the government vis-à-vis domestic security matters and providing more-general intelligence, the DCRG, with its regional structure, also plays an important role in informing the *préfets* [prefects] of the 96 regions of France. The *préfets* have strong regional powers and significant regional security responsibilities, so this is a critical role.

In practical terms, the DCRG gathers intelligence on terrorism originating internally, such as from domestic political extremists or Corsican, Basque, or Breton separatists; the DST, however, counters terrorism originating in or inspired from abroad. This division of missions and responsibilities is blurred when it comes to countering Islamist terrorism, which—though inspired from abroad—has regularly involved French nationals, including some converts. Consequently, this particular threat has been designated as a shared responsibility for the DCRG and the DST, and this has led to significant overlap, operational confusion, and tension between the two organizations. Most recently, these problems were highlighted when the DST arrested a group of Islamist suspects in northern France while the DCRG was still actively developing associated operational intelligence. This led to significant friction between the two organizations.[16]

The missions of the DST and the DCRG require those organizations to gather, process, and evaluate intelligence; maintain internal security; and protect classified documents and technology. Recently, DST responsibilities have been expanded to encompass new threats, such as the proliferation of chemical, biological, radiological, and nuclear weaponry and large-scale organized crime. To achieve their missions, both the DST and DCRG use open-source intelligence—including publications, papers, and speeches—and overt contacts (often key individuals in local communities). They also obtain covert intelligence through HUMINT from informants and sources; surveillance operations; and telephone, technical, and postal interception.

---

[15] Author interview with a UK policing and intelligence expert (and former Anglo-French liaison officer), October 2007.

[16] Author interview with a UK policing and intelligence expert (and former Anglo-French liaison officer), October 2007.

In fact, the DCRG "prefers to work through human informants or sources" (Cettina, 2003, p. 80). These shared techniques provide the DST and the DCRG with an opportunity for cooperation, but the two organizations have traditionally operated independently. Indeed, as has been previously mentioned, significant operational overlap has sometimes led to friction and rivalry. Although much of both organizations' current intelligence-gathering work is directed primarily at extremists in the substantial French Muslim community, the DCRG uses those capabilities against the domestic threats of Basque, Breton, and Corsican nationalist extremism and terrorism.

The DST also receives intelligence from other French intelligence services, such as the external foreign intelligence service (the DGSE), the police intelligence service (the DCRG), and the Direction du Renseignement Militaire [Military Intelligence Directorate] (DRM), and from foreign intelligence services. While these sources include the usual "friendly" services of other European countries and the United States, the DST also has good working relationships with other francophone services—notably, those of Algeria and Morocco. In addition, the DST is a member of the Kilowatt Group, a long-standing cooperation of Western intelligence services, and the Club de Berne, which brings together the heads of the various European intelligence organizations to discuss shared security concerns (see Baud, 2005).

DST and DCRG intelligence, the organizations' assistance during investigations, and the information the organizations provide to government, senior officials, and regional *préfets* is also used to inform the threat *niveaux* [levels] of the Vigipirate Plan, whose color-coded system of threat levels calls for additional physical security measures at CI and public and symbolic locations (see UCLAT, 2005). Introduced by the Secrétariat Général de la Défense Nationale [General Secretariat of National Defense] (SGDN) in 1978,

> the Vigipirate Plan was activated for the first time in January 1991, during the Gulf War. It was reactivated since then repeatedly: during summer 1995 following murderous terrorist attacks in Paris; in December 1996 after the attack committed in the Parisian RER, at the station Port Royal. It was again reactivated on

> Wednesday, September 12th, 2001 following the terrorist actions committed in the United States. (See UCLAT, 2005, p. 2.)

In March 2003, French authorities implemented a revamped Vigipirate Plan that allows far greater flexibility and is similar to the color-coded threat- and response-level systems used by many other countries.[17] Since its introduction, the new system has generally remained at *niveau orange* [level orange], except for several occasions (i.e., the Madrid train bombings of March 2004, the 60th anniversary of D-Day in June 2004, and the London bombings of July 7, 2005) when it was temporarily raised to *niveau rouge* [level red]. Additional plans are tailored to counter specific types of incidents: *biotox* [biological], *piratox* [chemical], *piratome* [nuclear], *piratair* [aircraft hijacking], *pirate-mer* [maritime], and *piranet* [cyberterrorism]. Disseminated intelligence reports on internal terrorism threats from both the DST and the DCRG play a critical role in assessing the threat level that directly informs the Vigipirate Plan.

In terms of the separation of intelligence and policing powers, the DCRG currently has no judicial powers; its previous powers of arrest applied only to horse racing and gambling. With the amalgamation of the DCRG and the DST, these powers were passed to the Police Judiciare, so the DCRG's current role is to perform intelligence gathering and relay its processed intelligence to other bodies for further action. The DST has the same arrest powers as the Police Judiciare, but it does not regularly use them. (An exception is a DST unit known as the Unite d'Enquete Judiciare [Judicial Investigation Unit], which is used specifically in arrest roles in CT and counterespionage.[18]) Nevertheless, to carry out the arrest phase of an intelligence-led CT operation and conduct investigative inquiries, the DST often works with the Sous-Direction Anti-terroriste [Anti-Terrorist Sub-Directorate] (SDAT)[19] of the Police Judiciare, or the Section Anti-terroriste [Anti-Terrorist section] of the Brigade Criminelle [Criminal Brigade] of the Paris police.

---

[17] See UCLAT, 2005, p. 3, for greater detail on the system of color-coded alert levels.

[18] Author interview with a senior French intelligence official, October 2007.

[19] Which, until June 2006, was known as the Division Nationale Anti-terroriste [National Anti-Terrorist Division] (DNAT).

Leadership and Human Capital

Since the appointment of its first (and charismatic) director, Roger Warin, who ran the organization until 1959, the DST has been considered the elite of the French Police Nationale, from which its staff are seconded. The DCRG likewise recruits its officers from pools of experienced police officers. This also occurs at the upper levels: Both organizations tend to recruit senior police officials for leadership positions. Although the secondment of specialists to the DST and the DCRG from other French military and security organizations occurs, this seems to be more common in France's external intelligence organization, the DGSE, where military personnel with specialist linguistic, cultural, and technical skills are seconded as required for specific operational roles.[20]

Following the election of President Nicolas Sarkozy, Bernard Squarcini replaced Pierre de Bousquet de Florian as director of the DST. A Corsican nicknamed *le Squale* [the Shark], Squarcini is a career policeman who specializes in CT and was the deputy director of the DCRG, which he was tasked to absorb into the DST to form DCRI.[21]

Although details of the two organizations' personnel and structure are sparse due to a *secret de defense* [defense secret] classification, it is known that the DST has approximately 1,600–1,800 staff. The DCRG, with its larger role and greater breadth of responsibilities, has 3,000–3,500 staff. The newly proposed DCRI will combine all the DST staff with approximately 80 percent of the DCRG staff, resulting in a staff of roughly 4,500. The remaining 20 percent of the DCRG will go either to the Sécurité Publique [Public Security] or the Police Judiciare.

---

[20] Author interview with former French military specialist, May 2008.

[21] See "Key Relationships with Other Intelligence and Law Enforcement Agencies" later in this chapter.

Management and Process

As France's domestic intelligence and internal security organizations, the DST and the DCRG have traditionally been under the management and control of the Ministère de l' Intérieur. Within the ministry, both the DST and DCRG are managed by the Inspection Générale de la Police Nationale [General Inspectorate of the National Police] (IGPN); while both organizations are free to identify and direct their resources against particular threats, the IGPN has both a management and an oversight role and carries out internal inquiries on matters of concern (such as recent questions about why DCRG was tasked to investigate Bruno Rebelle, one of Ségolène Royal's counselors, during the French presidential election).[22]

The DST can carry out its own independent intelligence inquiries and approach the judicial authorities to begin a judicial investigation, but many of its operations are initially instituted, then managed, through the French legal system's ongoing investigations into terrorism. This legal system, which is based on an inquisitorial structure common to many continental European countries, is significantly different from the adversarial legal systems found in the UK and the United States; it relies on inquisitorial magistrates to direct investigations and manage, through rogatory commissions, the various associated policing and intelligence bodies. While the emphasis in the adversarial British and U.S. legal systems is on establishing whether the defendant is guilty through zealous advocacy from both the prosecution and the defense, the inquisitorial French system places more emphasis on searching for and establishing the facts of the case.[23] Effectively, this legal system relies on the *juge d'instruction* [investigating magistrate], who conducts

> an impartial investigation to determine whether a crime worthy of prosecution has been committed. Once that determination is made, the investigating magistrate hands the case over to a prosecutor and a defence attorney, who, on the basis of the magistrate's

[22] Author interview with a senior French intelligence official, October 2007.

[23] For more details, see Vercher, 1992.

> investigation, act as advocates in front of a judge. (Shapiro and Suzan, 2003, p. 78.)

Due to the French policy of centralization, the specialist *juge d'instruction* of the 14th Section in Paris leads such investigations. Following the September 1986 introduction of a law pertaining to the fight against terrorism and the attacks on state security (*Décret n° 86-1020*), which still forms the bedrock of French CT legislation, the French authorities decided to centralize terrorism-related cases under the 14th Section of the public prosecutor's office in Paris. Consequently, terrorism cases, regardless of where in the country the incidents occur, are passed to the office of the 14th Section at the Galerie Saint-Eloi in the Palais de Justice where they are given to one of the four *juges* specializing in such cases. Due to the inquisitorial nature of the French legal system, the judges not only review the evidence and intelligence regarding the case, as in an adversarial legal system, but proactively direct and manage the various law enforcement and intelligence organizations as they investigate and develop the evidential case.

Such investigations and the intelligence and evidence they develop allow the judge to take advantage of the law pertaining to *association de malfaiteurs* [conspiracy in connection with a terrorist undertaking].[24] Introduced after the GIA bombings via Décret n° 96-647 on July 22, 1996, this law allows up to six days for the detention and interviewing of an individual believed to be involved in terrorism; after that time, the resultant file goes to the judge. If there is evidence of association in a terrorist conspiracy, the individual can be administratively detained for up to four years (two years in the case of a normal crime), while the judge carries out the investigation.[25] This process

> has proven to be an invaluable tool for the services of the *Police Judiciaire* and has become the fundamental legal justification for their activity. Without it, the management of Islamist terror-

[24] For more details of such legislation, see Gozzi, 2003.

[25] Author interview with a UK policing and intelligence expert (and former Anglo-French liaison officer), October 2007.

> ism since 1994 would not have been as effective. (Cettina, 2003, p. 87.)

Such judicial powers have been strengthened following the events of 9/11 by the introduction of a *loi sur la sécurité quotidienne* [day-to-day security law] introduced on November 15, 2001. Consequently, and given the nature of the French legal system, each judge develops not only an unprecedented knowledge of such cases but also strong relationships with the DST and other law enforcement and intelligence organizations (see Chalk and Rosenau, 2004). In contrast, the DCRG, which does not operate under a rogatory commission or warrant of investigation, has a purely intelligence-gathering role: Once it has processed its intelligence, it sends a report up the chain of command for further action.

As previously mentioned, due to overlap in DST and DCRG roles, particularly in relation to Islamist extremism and terrorism in France, there has been a significant lack of coordination and cooperation between the DCRG and the DST. Indeed, a lack of coordination has existed among all the French intelligence and law enforcement bodies involved in CT (see Shapiro and Suzan, 2003). This problem was further compounded by incidents of obstructionism and outright hostility between the DST and the DGSE (see Porch, 1997, pp. 422–454). One example of such hostility was evident in the fact that DST verified that telephone numbers obtained by New Zealand police who were investigating the sinking of the Greenpeace ship *Rainbow Warrior* in Auckland Harbour in 1985 belonged to the Ministère de la Défense (see Porch, 1997, p. 461).

As a consequence of these rivalries and the lack of coordination, a CT coordinating body was established and given a management role over the various official French bodies involved in CT, including the DST and the DCRG. The Unite de Coordination de la Lutte Anti-terroriste [Coordination Unit for the Anti-Terrorist Struggle] (UCLAT) (see DGPN, 2003) was established in 1984 within the Ministère de l'Intérieur. UCLAT is answerable to the Comité Interministériel de Lutte Anti-terroriste [Interministerial Committee for the Anti-Terrorist

Struggle] (CILAT)[26] and is led by the Police Nationale in the expectation that this structure will better coordinate the various organizations responding to terrorism. Consequently,

> UCLAT connects all the services involved in dealing with terrorist problems, bringing their representatives together once a week. The unit intervenes in specific terrorist cases by ensuring the relevant information changes hands . . . . It distributes intelligence to the services and encourages them to rise above any rivalry and share information. (Cettina, 2003, p. 83.)

Therefore, among various other organizations involved in countering terrorism, UCLAT has some level of control over the DST and the DCRG. One of the problems of this role for UCLAT is that, because it resides under the control of the Ministère de l'Intérieur and is not interministerial, it cannot directly issue orders to organizations under the control of either the foreign or defense ministries. It has also been suggested that the organization is too small, and that it requires more staff to be truly effective in its role.[27] Consequently, UCLAT sometimes has to rely on negotiation and persuasion, though this may change because President Sarkozy has expressed his desire for the organization to become an interministerial body.[28] Also coordinating intelligence under the control of the Ministère de l'Intérieur is the Conseil du Renseignement Intérieur [Interior Intelligence Council], which brings together representatives of the DST, the DCRG, and the Service de Coopération Technique International de Police [Service for Police International Technical Cooperation], which coordinates French international police liaison officers (see Baud, 2005, pp. 243–244).

---

[26] For details, see "Oversight" later in this chapter.

[27] Author interview with a UK policing and intelligence expert (and former Anglo-French liaison officer), October 2007.

[28] Author interview with a senior French intelligence official, October 2007.

Organizational Structure and Funding Patterns

Although the finer organizational details and staffing of the DST are classified, it is clear that a number of general structures, described below, fall under the director of the organization and his or her immediate counselors.

Under the central DST and its headquarters in Paris is a cabinet charged with national and international relations. There are also five operationally based sub-directorates that deal with (1) counterespionage, (2) international terrorism, (3) the security and protection of assets and technology, (4) technical administration, and (5) general administration. In the provinces, the DST is represented by the following six regional directorates (subdivided into brigades), all of which have the same competencies and areas of responsibility as the headquarters: Lille, Rennes, Bordeaux, Marseille, Lyon, and Metz. The DST is also represented in France's overseas departments and territories through its four posts: Antilles-Guyana, Réunion, Polynesia, and New Caledonia. Finally, the DST subdirectorate for economic security and the protection of national assets has units in 22 regions. These units protect French technology in various fields, including defense, telecommunications, chemicals and pharmaceuticals, private aviation, and computer technology.

Key Relationships with Other Intelligence and Law Enforcement Agencies

As was previously mentioned, the DST has close working relationships with a number of other French intelligence and policing organizations, including the following:

- the DGSE, which is subordinated to the Ministère de la Défense and is responsible for external intelligence gathering, searching and exploiting intelligence that is relevant to the security of France, and detecting and finding external espionage activities directed against French interests in order to prevent their consequences

- the DRM, whose primary purpose is to assist the Ministère de la Défense in matters of military intelligence. It integrates liaison officers into the Direction Générale de la Gendarmerie Nationale [General Directorate of the National Gendarmerie], the Direction de la Protection et de la Sécurité de la Défense [Directorate for Protection and Defense Security] (which is responsible for military security), and the Délégation Générale pour l'Armement [General Delegation for Armament] (which is responsible for technological military intelligence). The DRM also oversees the Helios space-satellite program. DRM headquarters are in Paris, but the organization has technical bases in Creil in the northern region of Oise and numerous other locations in both mainland France and its overseas territories.
- the DCRG, whose various domestic intelligence roles have been previously detailed. The organization has a headquarters, four *sous-directions* [subdirectorates], and numerous offices across the country (23 *directions régionales* [regional directorates] and 99 *directions départementales* [departmental directorates]), each of which fulfills many of the same competencies. The DCRG has also recently been involved in the establishment of regional centers comprised of local task forces of specialists from the DCRG, social security, immigration, and customs. These centers, located in 22 regions, are mandated to monitor and counter radicalization through the "Al Capone approach": That is, they look for financial, tax, and health and safety breaches as a means of curtailing extremism in local mosques. However, these centers have no specific judicial authority, and, consequently, the authorities are awaiting the first test case to establish some level of legal precedent.[29]
- the Traitement du Renseignement et Action contre les Circuits Financiers Clandestins [Treatment for Intelligence and Action against Clandestine Financial Circuits] and the Direction Nationale du Renseignement et des Enquêtes Douanières [National Directorate for Intelligence and Customs Enquiries], which provide economic intelligence and oversight among the

[29] Author interview with a senior French intelligence official, October 2007.

various French intelligence organizations vis-à-vis both organized crime and terrorist funding.

The DST also liaises with the Police Nationale (see Fairchild and Dammer, 2001, Chapter 5), which is responsible for policing urban areas, and the Gendarmerie Nationale (see Bertin, 1998; BLAT, 2005), which is responsible for policing rural areas, particularly when an operation enters its executive phase and arrests are necessary. Most of these actions are coordinated by UCLAT.

As was previously noted, the mandate and focus of the DST are predominantly concerned with foreign nationals who pose a threat within France and with terrorism inspired from abroad; the DCRG, on the other hand, is focused on French nationals involved in internal subversion and on domestic "homegrown" terrorism. However, as previously discussed, there is clearly a great deal of operational overlap, particularly in the organizations' shared responsibility for countering the growing threat posed by Islamist terrorism. Although both organizations technically form part of the Police Nationale and are thus under the control of the Ministère de l'Intérieur, there has been a history of duplication and rivalry, and even outright hostility, between the two groups. This problem has been aggravated by the existence of (1) SDAT, a third national police body tasked with the investigation of terrorist offenses, and (2) the semi-independent Paris prefecture of police, with its own CT policing subdivisions (the Renseignements Généraux de la Préfecture de Police de Paris [General Intelligence of the Paris Police Prefecture] and the investigative Section Anti-terroriste [Anti-Terrorist Section] of the Brigade Criminelle).

The DST and the DCRG are currently being amalgamated with the SDAT at a new headquarters building in Levallois-Perret, Hauts-de Seine, just outside of Paris. It was reported that the organization would be named "Direction Central de Renseignements Interieure" (Smolar, 2006).[30]

[30] Author interview with a senior French intelligence official, October 2007.

Oversight

Unlike most contemporary intelligence organizations in Europe,[31] the DST, DCRG, and French intelligence organizations in general are not currently overseen by Parliament. Indeed, there is a distinct lack of formal oversight of French intelligence organizations relative to many of their European counterparts. Despite the Anti-Terrorist Law of January 23, 2006, which raised the issue of parliamentary oversight, and the report of Sénateur René Garrec, which recommended such a measure, the French intelligence organizations have historically rejected this form of oversight. Much of this resistance is due to history: "In France, the role and ideological allegiances of the Communist Party during the 'Cold War' without doubt contributed in blocking the tentative installation of a parliamentary control" (Baud, 2005, p. 245). This history led to a November 17, 1958, order forbidding all parliamentary commissions from accessing secrets concerning national defense, foreign affairs, and interior and exterior security. However, in November 2005, then–Ministre de l'Intérieur Nicolas Sarkozy publicly declared the need to establish parliamentary control over French intelligence services. Subsequently, at the end of 2006, Premier Ministre Dominique de Villepin presented the French Parliament with a project to introduce a law for the creation of a parliamentary delegation for intelligence. This commission to control the intelligence services was to comprise three *senateurs* from the Sénat [the Upper House] and three *députés* from the Assemblée Nationale [the Lower House] who would work under the protective security classification *secret de la défense nationale*.[32]

A law passed on September 25, 2007, finally established the need for parliamentary control over the French intelligence services, and the politicians to be involved will be appropriately vetted.[33] Surprisingly, the main drive for the establishment of political oversight is coming from the intelligence services themselves, which no longer view such oversight as problematic and in fact want the political and judicial

---

[31] With the possible exception of the Portuguese intelligence services.

[32] Details are based on Zamponi, 2006, p. 386.

[33] Author interview with a senior French intelligence official, October 2007.

cover and legitimacy for their operations that such oversight would provide.[34] Unfortunately, unlike some in other Western nations, many in the French political classes see intelligence as a contentious subject that will not further their political careers and, consequently, some politicians may not want to be involved in its oversight. Even when such political oversight is successfully established, France's history and fears that such oversight might limit an organization's capacity for action (see Baud, 2005, p. 245) make it likely that any control and oversight will be "light."[35]

At present, oversight of the intelligence services is mainly administrative. At the uppermost strategic level is the Conseil de Sécurité Intérieure [Council for Interior Security], which, since 1997, has allowed the prime minister and other relevant senior ministers to discuss and evaluate various potential threats and modify the country's security organizations appropriately. However, main responsibility for overseeing the intelligence services rests with the Ministère de l'Intérieur via CILAT, which meets roughly twice per year and provides a strategic and high-level oversight of the DST, the DCRG, and operational CT coordination generally. CILAT normally includes the prime minister, the minister of the interior, and other relevant ministers. CILAT is an interministerial committee but because it falls under the control of the Ministère de l'Intérieur and is associated with the police, it has more-limited powers of oversight when it comes to those intelligence and other CT organizations that fall under the control of the French army or the Ministère de la Défense.[36] The Comité Interministériel du Renseignement [Interministerial Intelligence Committee] is another interministerial committee with responsibilities for overseeing the DST and other French intelligence organizations. Created by ordinance on January 7, 1959, this committee brings together relevant ministers, the general secretary of the government, and the SGDN; consequently, it has greater control over military intelligence structures.

---

[34] Author interview with a senior French intelligence official, October 2007.

[35] Author interview with a senior French intelligence official, October 2007.

[36] Author interview with a senior French intelligence official, October 2007.

The SGDN acts as a secretariat for the various intelligence organizations, establishes the national intelligence plan, sets the objectives for the intelligence services, and distributes the financial resources allocated by the prime minister.[37] As was previously discussed, the French system of *juge d'instruction* also provides some level of judicial oversight of the DST. Consequently, it should be noted that although the DST tends to operate under a rogatory commission, the DCRG "does not require a rogatory commission and therefore has more freedom to act" (Cettina, 2003, p. 80).

Problems or Controversies

For many years, due to the number of PCF members involved in the French administration and various allegations of infiltration by Soviet agents,[38] the French intelligence services, including the DST, were not trusted or deemed reliable by their Western counterparts, particularly those in the United States. This led to significant cooperation problems during the Cold War. More recently, in relation to the French intelligence services' widespread use of informants and agents within the Muslim minority community in France has provoked concerns about the threat of Islamist infiltration into these services.[39]

Particularly during the postwar presidency of de Gaulle, the French nationalist agenda led to a number of major disagreements between the French intelligence services and their U.S. counterparts. In one of the more extreme examples, de Gaulle ordered the French services to break contact with the U.S. Central Intelligence Agency (CIA) from 1964 to 1967 (see Porch, 1997). More recently, and while France was supporting the post-9/11 intervention in Afghanistan (see McAllister, 2003) and

---

[37] There are also such commissions as the *Commission Consultative du Secret de la Défense Nationale*, which is responsible for the declassification of documents, and the *Commission Nationale de Contrôle des Interceptions de Sécurité*, which is responsible for oversight of security interceptions. For more details, see Thuillier, 2000, p. 118.

[38] For detailed analysis of this issue, see Andrew and Mitrokhin, 2001, Chapter 27 (see also Faligot, 2006a).

[39] Author interview with a senior French intelligence official, October 2007.

providing specialist military forces there (see Micheletti, 2003), political tension between the two countries developed over the 2003 invasion of Iraq. However, despite such strategic political disagreements, bilateral cooperation among intelligence and CT organizations in the two countries has been maintained and indeed enhanced with the formation of a joint CT intelligence center known as Alliance Base. Established in Paris by the DGSE, the CIA, and other intelligence agencies, this international fusion center was allegedly involved in France's arrest of Christian Ganczarski, a German national associated with al Qaeda and linked to the April 2002 suicide attack on a synagogue in Djerba, Tunisia.

During the French war in Algeria between 1954 and 1962, there were numerous reports of France's use of torture and extrajudicial executions (see Aussaresses and Miller, 2006; Kauffer, 2006a). While many of these historic human-rights abuses have been linked to the French military, the DST and other French intelligence services charged with countering the FLN have been accused of using such methods; this historical legacy thus taints the organization (see also Delaporte, 2003). In addition, allegations have been raised that the DST was involved in coordinating false-flag terrorist attacks during the conflict in pursuit of its longer-term political objectives.[40]

There have been scandals regarding French authorities' use of the intelligence services to monitor legitimate domestic political opposition. Perhaps one of the best-known incidents occurred in 1973, when DST telephone taps were discovered in the offices of the satirical left-wing magazine, *Le Canard Enchaîné.* The resulting scandal and debates about spying on other French nationals for political purposes ended in the resignation of the then–Ministre de l'Intérieur Raymond Marcellin (see Porch, 1997). There have also been concerns that leading politicians have used sensitive intelligence to bolster their arguments during political debates. This "politicization of intelligence," which has clearly occurred in other countries, has been apparent in France.

---

[40] See Faligot and Krop, 1999. A *false-flag operation* is a covert government, corporate, or other operation designed to look like another entity actually perpetrated it.

French politicians' previous distrust of regular intelligence organizations has historically caused these politicians to turn to parallel organizations. In perhaps the most extreme example of this phenomenon, President François Mitterrand established the Cellule Antiterroriste de l'Élysée [the Anti-Terrorist Cell of the Elysée] in 1982 and placed it under the command of Christian Prouteau, the head of the GIGN, to head up the response to terrorism. Mitterrand's left-wing political background caused him to distrust the traditional French intelligence services and set up his own intelligence structure based in the gendarmerie, which the French see as an apolitical organization.[41] This new structure caused significant concern because the GIGN's primary role was tactical intervention, not intelligence. Indeed, the cell was ultimately charged with false arrests and fabricating evidence after it arrested three Irish nationals and falsely accused them of terrorism (see Porch, 1997, Chapter 18).

It has been alleged that, due to their historical legacy and roots in the Resistance movement of World War II and France's traditional association of intelligence and action, French intelligence organizations have a tendency to use "operational" covert action responses by such groups as the DGSE's Service Action [Action Service—i.e., a direct-action team] (SA) and the former 11e Régiment Parachutiste de Choc [11th "Shock" Parachute Regiment] to provide a direct-action solution to ongoing intelligence problems. Critics cite the July 1985 sinking of the Greenpeace *Rainbow Warrior* in Auckland Harbour, New Zealand, as an example.[42] This DGSE operation resulted in the death of a photographer, the arrest and trial of DGSE SA officers Major Alain Mafart and Captain Dominique Prieur, and the resignations of Ministre de la Défense Charles Hernu and the director of the DGSE, Admiral Pierre Lacoste (see Porch, 1997, Chapter 19).

One final concern that has been raised about countering Islamist extremism and terrorism in France is the use of large-scale roundups and the indiscriminate detention of Muslim suspects. During Operation Chrysanthemum on November 9, 1993, for example, 88 Muslims

---

[41] Author interview with a senior French intelligence official, October 2007.

[42] For details of the operational structure, see Baud, 1998.

were detained and questioned but only three were eventually incarcerated and placed under investigation for "conspiracy in relation to a terrorist enterprise" (see Shapiro and Suzan, 2003, p. 84). The French authorities argue that such roundups are essential to countering Islamist terrorist networks (particularly those that provide support and funding) but the operations have been condemned by civil rights groups and have led to significant tensions with the Muslim community.

Conclusion

While France has a great deal of experience in countering both terrorism and insurgency, it inherited a dual-institution domestic intelligence structure shaped by historical circumstances—most notably, the fissure in French society caused by the split between the Vichy and Free French regimes during World War II. Despite (or perhaps because of) different origins, structures, and roles—and although the DCRG focuses on more-general intelligence that originates domestically while the DST concentrates on domestic threats that originate abroad and the activities of foreign nationals within France—an inevitable level of overlap, duplication, and friction have arisen between the two organizations. Consequently, and despite greater centralization and coordination of CT activities (particularly since the establishment of UCLAT in 1984 and the introduction of *Décret n° 86-1020* in 1986), such factors have often caused problems at the operational level.

At the same time, the nature of the terrorist threat has mutated: The comparatively clearly defined domestic nationalist and left- and right-wing extremist groups; international, state-sponsored organizations; and political organizations that used to be the major concern are taking a second seat to the global ideological terrorist network of Islamist extremists. At an overarching level, this change in the nature of terrorism has blurred and broken down the traditional barriers between domestic and international, internal and external, and homegrown and transnational threats.

In the case of French domestic intelligence structures, this mutation has increased the overlap between the DST and the DCRG.

This blurring is exemplified in the task of identifying organizational responsibility for countering French-born nationals, some of whom are second- or third-generation Muslims of North African origin or white converts, who are involved in terrorist conspiracies within France but clearly belong to the wider international Islamist network. In theory, both the DST and the DCRG could claim primacy in such cases. Consequently, and to better address the changed current situation, the French authorities have taken the major decision to sidestep historical inertia by amalgamating the two organizations into the DCRI. Only time will tell how effective this new domestic intelligence structure will be in countering terrorism, but it already enjoys the advantages realized by combining the significant operational experience and expertise of the DST and DCRG with the investigative skills of the SDAT into a single, centralized domestic intelligence body with clear national primacy.

CHAPTER FIVE

Germany

Richard Warnes

Among Western nations, Germany has a unique domestic intelligence structure in which numerous independent intelligence agencies reflect the national administrative structure of the 16 national *Länder* [states].[1] While the Bundesamtes für Verfassungsschutz [Federal Office for the Protection of the Constitution] (BfV) has an overarching federal role based in both historical legacy and the concept of *Trennungsgebot* [principle of separation], its primary role is to facilitate cooperation and coordination rather than exercise any direct legal control or powers over the 16 state-based Landesämter für Verfassungsschutz [regional intelligence organizations] (LfVs), which are equal in status to the BfV. Thus, much of what follows in relation to the BfV is equally applicable to the various LfVs.

Creation and Relevant History

In 1949, the Allied occupying powers in Germany sent the new West German authorities a "police letter" that gave them the authority to establish an organization to counter subversion. Based on the model of the UK's MI5, the letter specified that there had to be a clear division between such an intelligence organization and police powers. Consequently, *Trennungsgebot* developed. This led not only to the separation

[1] The sixteen separate *Länder* are the regional components within the German federal system. Ten *Länder* were formed from West Germany, five from East Germany. The final *Land* [state] is Berlin.

of intelligence and policing powers as in the UK model but also to a division of powers between the federal and *Land* levels. The BfV was thus established under the Bundesministerium des Innern [Federal Ministry of the Interior of the Federal Republic of Germany] (BMI) by the Bundesverfassungsschutzgesetz [Federal Law for the Protection of the Constitution] (BVerfSchG) law of July 28, 1950, following the division of Germany into two states, the Federal Republic of Germany (FRG) and the German Democratic Republic (GDR), in the immediate postwar period. The BfV's initial role was to counter espionage in the FRG in response to the threats posed by the potential of revived Nazism and by communist activists working for the Hauptverwaltung Aufklärung [East German administration] (HVA) (see Andrew and Mitrokhin, 2001, Chapter 26), led by General Markus Johannes "Mischa" Wolf of the GDR Ministerium für Staatssicherheit [Ministry for State Security] (MfS) (see Baud, 1998).

Having initially been established to monitor the threats posed by revived postwar Nazism and East German infiltration during the Cold War, the BfV played a key role in countering the extreme-left-wing domestic terrorist threat that emanated during the 1970s and 1980s from such organizations as the Baader-Meinhof Gang, which developed into the Rote Armee Fraktion [Red Army Faction] (RAF), the Bewegung 2. Juni [Movement 2 June], the Revolutionäre Zellen [Revolutionary Cells], and Rote Zora [Red Zora, an extreme left-wing, all-female terrorist group] (see Horchem, 1991, 1993).

The RAF in particular was responsible for a number of bombings and numerous attacks against prominent German officials, including the assassinations of Siegfried Buback, the Generalbundesanwalt [chief federal prosecutor], on April 7, 1977, and Jürgen Ponto, chair of the Deutsche Bank, on July 30, 1977, and the October 1977 kidnapping and murder of Hanns-Martin Schleyer, president of the German Employers Association and a leading industrialist. Later assassination victims included Ernst Zimmerman, a defense industrialist; Karl-Heinz Beckurts, head of research at Siemens; Gerold von Braunmühl of the foreign ministry; and Alfred Herrhausen, head of the Deutsche Bank, in 1989. The group's final assassination target was Detlev Karsten Rohwedder, the head of the Treuhandanstalt [the office responsible for the sale of

East German state assets following the reunification of Germany], which was responsible for the privatization of state industries in former East Germany, in the spring of 1991 (see Rojahn, 1998). Further RAF attacks targeted U.S. military personnel and bases[2] and included assassination attempts against General Alexander Haig on June 25, 1979, and General Frederick Kroesen on September 15, 1981; the bombing of the U.S. Air Force base at Ramstein on August 31, 1981; and the kidnapping and murder of Spc. Edward Pimental on August 7, 1985, in order to obtain his identity card and thus gain access to Rhein-Main Air Force base with a car bomb. This bomb exploded the following day, killing two and wounding 11.[3]

While responding to domestic terrorism perpetrated by extreme-left-wing groups, the BfV also began countering the threat posed to Germany by international politically motivated terrorism, which developed in the early 1970s and whose most notable instance was the Black September kidnapping and murder of Israeli athletes at the Munich Olympic Games in 1972 (see Reeve, 2006). As a result of the failed police rescue bid, the West German authorities formed the Grenzschutzgruppe 9 [Border Guard Group 9, an elite tactical intervention unit] (GSG 9) (see Tophoven, 1977) intervention unit from the Bundesgrenzschutz [federal border guards] (BGS) (see Meyer, 2001). Consequently, when the Popular Front for the Liberation of Palestine–Special Operations Group (PFLP-SOG) hijacked a Lufthansa jet on behalf of the RAF[4] in October 1977, it was GSG 9 commandos who led Operation Fire Magic, which resulted in the successful rescue of the hostages in Mogadishu (see Harclerode, 2000, Chapter 7).

Following the removal of the Berlin Wall, the collapse of the Soviet Union, and the reunification of Germany in 1990, the BfV was also tasked with monitoring the theft and export of sensitive indus-

---

[2] Author interview, October 2007. A senior BfV intelligence official pointed out that, along with their other national security considerations, the German authorities must constantly bear in mind the security of U.S. and UK military bases.

[3] For a detailed examination of the RAF campaign of attacks, see Peters, 2004.

[4] For details of the historical collaboration between German extreme-left terrorists and Palestinian terrorists, see Karmon, 2000.

trial material and technology. The revival of neo-Nazi groups and the skinhead movement in Germany in the early 1990s led to increased surveillance and monitoring of such groups and the concomitant expansion of staff in the BfV (see Schmidt, 1993). However, due to the "leaderless resistance" of the neo-Nazis and the multiplicity of groups involved, this surveillance and monitoring initially proved difficult. As Eckart Werthebach, president of the BfV at the time, stated, "We cannot simply infiltrate a liaison man into the leadership, because there is no leadership. We must use small networks that reach into the small groups and cliques" (see "Werthebach Views Threat from Extremism," 1993). Nevertheless, the BfV's longer-term success at recruiting informants in the largest neo-Nazi party, the Nationaldemokratische Partei Deutschlands [German National Democratic Party] (NPD), was later disclosed during a controversial court case in 2002 (see Cleaver, 2002a). In 1992, just as the threat posed by such German neo-Nazism was increasing (see Anderson, 1995), the RAF issued a unilateral cease-fire, effectively ending its operational campaign (see Pluchinsky, 1993).

Most recently, the BfV has become actively involved in monitoring the threat posed to Germany by Islamist extremism and the al Qaeda network, particularly following the al Qaeda Frankfurt cell's planned attack on the Strasbourg Winter Market in December 2000 (see Connolly, 2003; Boyes, 2003). This role increased dramatically following the discovery that Mohamed Atta and his colleagues had used Hamburg as a base before the 9/11 attacks (see Gunaratna, 2003; Wright, 2006) and had received support from Mounir El Motassadeq (see Cleaver, 2002b). These foreign nationals used Germany as a base while Islamists in other countries have targeted German tourists traveling abroad. In Djerba, Tunisia, on April 11, 2002, 14 German nationals died along with seven other people after a propane tanker was crashed into the synagogue they were visiting (see "Is Germany Next on the Terrorists' List?" 2002). In Algeria in 2003, a number of Germans were kidnapped along with other Europeans (see Paterson, 2003) by a group linked to GSPC.[5] Consequently, fears increased that

[5] At the start of 2007, the GSPC announced its new name: Al Qaeda in the Islamic Maghreb (see Schanzer, 2004).

Germany's active military involvement in Afghanistan (see Micheletti, 2003) might make the country and its citizens targets. German military forces certainly have been directly targeted: Two suicide attacks targeted Bundeswehr [federal army—i.e., the German army] soldiers in Kabul on June 2, 2003, and November 14, 2005, and two GSG 9 members were shot during a convoy ambush near Fallujah, Iraq, on April 7, 2004 (see Stock and Herz, 2007).

The impact of this current type of Islamist threat on domestic German security and the potential for radicalization (see Uhlmann, 2005; Boukhars, 2007) are of particular concern to Germany, which has a sizable minority Muslim population of approximately 3.3 million, of which the largest groups are the Turkish and Kurdish communities, which number around 1.76 million persons total.[6] Such fears were heightened by the September 2002 arrest of a Turkish man and his American fiancée, who were believed to be planning an attack on U.S. military bases in Heidelberg (see Helm, 2002), the failure of a plot involving a Lebanese student in Kiel and an accomplice to simultaneously bomb two German passenger trains in Dortmund and Koblenz with homemade propane bombs in July 2006 (see Boyes, 2006), and the June 2007 arrest in Pakistan of three German Islamists participating in a group believed to be training for suicide bombings (see McHugh, 2007). Perhaps the greatest indication of the level of threat facing Germany was the September 4, 2007, arrest in Oberschledorn of three Islamic Jihad Union (IJU) associates (a Turkish man and two white German converts to Islam) who had 750 kg of hydrogen peroxide and were believed to be conspiring with up to seven others to attack the U.S. base at Ramstein, Frankfurt Airport, and various U.S. military social venues in Germany (see Boyes, 2007; Landler and Kulish, 2007; Campbell, 2007). This concern was reinforced when, on March 3, 2008, Cüneyt Ciftci, a 28-year-old Turkish national from Germany, drove a suicide truck bomb into a military post in Afghanistan, killing two U.S. soldiers and two civilians. The attack was believed to have been planned by Eric Breininger, a white German convert to Islam, and his Lebanese-born German colleague

[6] Figures courtesy of the BfV, provided in December 2007.

Houssain al-Malla, who are linked to the IJU cell and believed to be in the Pakistan-Afghanistan border region ("Analysis: German Suspects in Afghanistan," 2008).

Mission and Critical Capabilities

The BfV's task, laid down in law,

> is to monitor all activities directed against the free democratic order. It is responsible for counter-espionage [and] collects information on the activities of foreigners, where these pose a threat to security, and on the activities directed against international understanding. (BfV, 2007a.)

The phrase "activities directed against international understanding" has been more clearly defined in law as "Islamism and Islamist terrorism." To achieve its mission, the BfV monitors, observes, and develops and evaluates intelligence on those individuals and groups that pose a threat to the constitution and democratic system of Germany (see BfV, 2008). These are identified as left-wing and anarchist extremists and terrorists,[7] right-wing extremists and terrorists (see BfV, 2002, 2006b), foreign political extremists from within Germany's sizable minority groups who pose a threat to security,[8] and Islamist extremists and terrorist groups (see BfV, 2006a, 2007b).

The BfV is also tasked with countering espionage from foreign nations, protecting sensitive German intelligence and technical equipment and expertise, and vetting persons employed in sensitive military or government positions (and, since 9/11, of persons employed in essential industry and CI). Interestingly, the BfV includes the Scientology Organization among those organizations it monitors as "concrete evi-

---

[7] Some, such as the Kommunistische Plattform [Communist Platform], have emerged from the more mainstream Marxist-Leninist Partei des Demokratischen Sozialismus [Democratic Socialist Party] (PDS); others, such as Linksruck [Left Shift] and Sozialistische Alternative [Socialist Alternative], have a Trotskyist background.

[8] Including the PKK, the LTTE, and Sikh extremists.

dence [that] activities directed against the free democratic basic order continues to be available[;] this is why there is a legal requirement for the organization to be monitored" (see BfV, undated[a]). In 1997, after the BfV established that there were approximately 6,000 members of the Scientology movement in Germany, Scientology took the German authorities to court over the monitoring. The courts rejected the claim and confirmed the BfV's right to monitor the organization.[9] Finally, the BfV liaises and cooperates with other German intelligence and security bodies and those of its international colleagues, particularly in relation to the ongoing threat posed by Islamist terrorism, which "has developed into a major threat posed to the internal security of the Federal Republic of Germany" (see BfV, undated[b]). The specific missions assigned to the BfV are outlined in Section 3 of the BVerfSchG.

A large part of the information collected by the BfV (and the LfVs) is obtained from open sources, such as the written press, brochures, and public and political statements.[10] Other information is obtained through more-proactive covert intelligence gathering—in particular, through the infiltration or recruitment and handling of human sources, surveillance, various telephone and postal intercepts and covert searches; data collection from banks, postal services, airlines, and communication companies; and technical eavesdropping, photography, and video recording (see BfV, 2007a, Section 10). The final sources of information and intelligence are other German policing and intelligence organizations and friendly foreign intelligence organizations. To carry out covert surveillance, the head of the respective department must authorize the activity;[11] the use of interception or technical intelligence gathering requires prior authorization from both the BMI and the G-10 Commission, which was created by Article 10 of the *Grundgesetz* [Basic Law, effectively the German constitution] of

---

[9] Author interview with senior BfV intelligence officials, October 2007.

[10] Author interview, October 2007. A senior BfV intelligence official estimates that approximately 60 percent of intelligence comes from open sources, 20 percent from covert intelligence gathering, and 20 percent from Polizei [police], Grenzschutz [border police], banks, postal services, and other sources.

[11] Detailed in an untitled BfV memo of December 2007.

May 1949 (see "Oversight" later in this chapter). After 9/11, the BVerfSchG was amended to help the BfV's obtain bank-account details, airline passenger lists, postal information, and mobile and land-based telephone numbers. Although strong restrictions and controls still apply to these specific sources of data, since the beginning of 2007, the BfV has needed to obtain clearance only from the BMI.[12]

Once collated, evaluated, and interpreted by the BfV and the 16 independent regional LfVs, the resulting intelligence is entered into the organizations' intelligence database, the Nachrichtendienstliche Informationssystem [Intelligence Service Information System] (NADIS). This system allows both the BfV and the various LfVs to add information into a searchable database and to access the centralized data it contains. The NADIS database is searchable, but it identifies only the relevant file-registration number and general information; for details, the requester must obtain the file.[13] Due to *Trennungsgebot*, which, among other separations, promotes data protection by firewalling information, the Bundeskriminalamt [federal criminal police] (BKA) and the Landeskriminalamt [regional or state criminal police] (LKA) have no access to the NADIS database. Likewise, the BfV and LfVs have no direct access to the police organizations' databases, including the police information system, which allows a *Fahndung* [data check] by operational officers. Both these systems are firewalled and independently controlled, but a 2006 law established a joint intelligence and policing antiterrorism database. The effectiveness of such German databases in countering terrorism was demonstrated by the *Ziefahndung* [target searches] on the "Kommissar" computer via the Personen-Institutionen-Objekte-Sachen [people, institutions, objects, and places] index, which was used with some success by then–Director of the BKA Horst Herold to counter the RAF in the 1970s and 1980s (see Combs, 2006). Currently, technical specialists seconded from the relevant Bundesamtes für Sicherheit in der Informationstechnik [Federal Office for the Security of Information Technology] (BSI) maintain NADIS oversight, integrity, and confidentiality. A special federal law

[12] Author interview with a senior BfV intelligence official, October 2007.

[13] Author interview with a senior BfV intelligence official, October 2007.

of December 20, 1990, specifically defines the legislative basis, access, and limits of privacy for the databases,[14] but "the Federal Commissioner for Data Protection . . . controls observance of the provisions of the Federal Data Protection Act and other regulations on data protection by the BfV" (BfV, 2007a, Section 13).

The BfV provides important evidence for trials and convictions of individuals involved in terrorist or espionage activities but due to the policy of *Trennungsgebot*, it has no police powers of its own and cannot carry out arrests, searches, or confiscations of property (see Bennett, 2002). It also has no power to formally question suspects, although it can ask people to voluntarily provide information. Therefore, although the BfV cannot use such methods to investigate terrorist conspiracies or offenses, it clearly does collate, evaluate, and interpret information to develop actionable intelligence. Consequently, the BfV disseminates its processed and evaluated intelligence to appropriate German federal and state policing agencies, such as the BKA, BGS, and appropriate Landespolizei [state police], that do have executive powers.[15]

The BfV also disseminates its processed intelligence to other agencies of the German government, providing them with an overview of potential threats to security and the opportunity to introduce appropriate defensive security measures. As well as informing the government's decisionmaking, such information and intelligence allows the Bundesverfassungsgericht [federal constitutional court] to ban a party or organization, remove the constitutional rights of an individual, and ban extremists from public employment. For example, the Bundesverfassungsgericht has banned both neo-Nazis and communist parties. In 2003, there were attempts to ban the NPD, one of the largest extreme-right-wing parties. Five judges agreed to the ban but three judges argued that there were too many BfV informants in leadership positions who may have acted as agents provocateurs; thus,

---

[14] Details of the NADIS and INPOL systems are based on information contained in Thuillier, 2000, pp. 17–18.

[15] Comprising the *Schutzpolizei* (Schupo) [uniformed police], *Kriminalpolizei* (Kripo) [criminal investigative police], and the *Bereitschaftspolizei* (Bepo) [public order police]. For more details, see Thuillier, 2000, Annex 1.

the required level of majority was not reached and the party was not banned. This decision opened a wider discussion in Germany about the need in a democratic society to ban or outlaw a party; at the same time, but at a more operational level, a dilemma emerged for the BfV: Should it stop using informants within an extremist party and increase the likelihood of that party being banned but lose vital intelligence on its actions? Or should it maintain good intelligence coverage of an extremist party through informants and risk having the Bundesvefassungsgericht reject a legal application for the party to be banned? The dilemma reaches beyond political parties because extremist organizations can also be banned. When such organizations are located within a single *Land*, the minister of the interior of the particular *Land* can ban them; if they are in two or more *Länder*, the responsibility for considering a ban belongs to the Bundesinnenminister [federal minister of the interior].[16] Thus, during the 1990s, many domestic neo-Nazi organizations were banned along with the PKK (see Dietl, Hirschmann, and Tophoven, 2006, pp. 51–57); more recently, the Islamist Hizb ut-Tahrir al-Islami [Islamic Party of Liberation] was banned along with the Kalifatstaat [caliphate state] of Metin Kaplan, which is based in Cologne.[17]

Note that because of the German domestic intelligence structure's multiple agencies and the fact that the BfV operates under federal legislation while the powers of the various LfVs derive from the state legislation of the various *Länder*,[18] the BfV and the 16 LfVs all have slightly different powers. For example, the BfV cannot use electronic means to bug a residence, but the LfVs do have such powers. Similarly, the BfV cannot store data on individuals younger than 16 years, but the age limit in Bavaria is 14 years. And while the BfV does not currently monitor organized crime, some LfVs do.[19] Thus, although the BVerf-

[16] Author interview with senior BfV intelligence officials, October 2007.

[17] See Karacs, 2001. Kaplan is currently serving a life sentence, having been extradited to Turkey.

[18] See "Organizational Structure and Funding Patterns" later in this chapter for more details.

[19] Author interview with senior BfV intelligence officials, October 2007.

SchG has regularly been amended and significantly expanded over the years, it is binding on the LfVs only in terms of their cooperation with other LfVs and the BfV.

Leadership and Human Capital

The president and vice president of the BfV are nominated by the BMI with the agreement of the Bundeskanzler [the head of the German government]. As of this writing, the BfV president is Heinz Fromm, who was previously the director of the LfV for Hessen, and the BfV vice president is Hans Elmar Remberg. Although it is an unwritten rule, an effort is often made to ensure that appointments to the top positions in the various German intelligence organizations reflect a political balance; thus, the political associations of appointees are considered.

As of 2006, the BfV had 2,447 staff. The majority are based at BfV headquarters in Cologne, but there is another large office in Berlin. Abteilung VI [Division 6], the subdivision responsible for Islamist extremism, is based in Cologne; the subdivision for Islamist terrorism is based in Berlin.[20] Like other German intelligence and security organizations, the BfV has felt increasing political pressure to centralize its headquarters in Berlin, closer to the seat of government. The 16 LfVs, on the other hand, have about 2,900 total staff, ranging from more than 400 employees in Bavaria's LfV to fewer than 50 in some of the smaller LfVs.[21]

The BfV also runs a training school, the Schule für Verfassungsschutz at Swistal-Heimerzheim [School for the Protection of the Constitution, essentially a domestic-intelligence school], which recruits from universities, offers training courses taken at different stages of a BfV member's career, and trains staff from the Militärische Abschirmdienst [Military Intelligence Service] (MAD) and the various LfVs.

---

[20] Detail from an untitled BfV memo of December 2007 (see also "Organizational Structure and Funding Patterns" later in this chapter).

[21] Author interview with senior BfV intelligence officials, October 2007.

Management and Process

As a domestic intelligence and internal security organization, the BfV is answerable and subordinate to the BMI. Article 16 of the BVerSchG establishes the BMI's role in managing the BfV and outlines three key areas of responsibility (see Thuillier, 2000):

- to exercise permanent supervision over the organization's intelligence missions
- to optimize efficiency
- to guarantee legality in the running and organization of its missions.

The BMI is also involved in the promotions and appointments of individuals to higher levels of the BfV, ultimately deciding on candidates' suitability for positions. It can also allocate special tasks to the BfV and monitors their progress.

Legislation strictly controls what processes BfV uses to carry out its missions. Relevant legislation includes the Grundgesetz promulgated by the Bundestag (legislature) on May 23, 1949; the BVerfSchG of July 28, 1950, which was reintroduced August 31, 1990, at the time of the drafting of reunification legislation; and the constitutional principle of *Trennungsgebot* (see Thuillier, 2000, pp. 26–28).

Organizational Structure and Funding Patterns

The Cologne-based BfV, which spent €137 million in 2006, has a federal role given its overarching responsibility for cooperation among intelligence agencies and the coordination of domestic intelligence. However, the key structure of German domestic intelligence is based on the network of 16 LfVs. Each LfV is an independent organization answerable to the minister of the interior of each *Land*, and although the BfV cannot give the LfVs any direct orders, a federal mandate under Article 73 ¶10 of the Grundgesetz requires cooperation between the BfV and the various LfVs. Consequently, while many LfVs will deal with local threats specific to their *Länder*, in the case of a wider con-

spiracy that involves more than one *Land*, the BfV will normally liaise with and coordinate its actions with or through the regional LfVs.

When the BfV wants to collect information in a particular *Land*, it must first secure the regional LfV's opinion and suggestions. Although a request for permission per se is not required, the LfV may suggest appropriate methods and offer to assist with the operation because its staff knows the local area and has suitable contacts. Much administrative work is therefore completed at the level of the *Länder*. Each LfV has the same range of competencies as the BfV but operates according to the particular threats in its *Land.* There are concerns that Germany's decentralized *Land*-based domestic intelligence architecture—and indeed its similar law enforcement structures—may adversely affect the overall system's operational capability. Such decentralized separation, enforced by legislation and based on the historical concept of *Trennungsgebot*, may affect strategic operational capability; it also clearly increases the likelihood that critical intelligence will fall through the cracks and that essential information sharing will be inhibited. Such concerns about information flows are exacerbated by legislative firewalls around interagency information sharing and strict data-protection controls.

In 2004, in an effort to centralize and better coordinate this historic structure, Otto Schily, the minister of the interior, attempted to put all of the LfVs directly under the control of one institution.[22] This move was rejected by the *Länder* and failed to get the two-thirds majority necessary in the Bundestag. Consequently, while most of the LfV offices are under the direct authority of each *Land*'s ministry of the interior, four of the LfVs are directly integrated into the ministries of the interior of their own *Land* and are therefore known as Innenministerium/LfVs [Ministry of the Interior LfVs] (see Thuillier, 2000). This distinction has no direct bearing on the size or role of these LfVs but merely reflects where they sit in the individual *Land* structure. The 16 LfVs are

[22] Minister Schily also sought unsuccessfully to integrate all the LKAs into the federal police BKA.

- LfV Niedersachsen (Lower Saxony)
- LfV Bremen
- LfV Hamburg
- IM/LfV Mecklenburg-Vorpommern (Mecklenburg–Western Pomerania)
- LfV Sachsen-Anhalt
- LfV Sachsen (Saxony)
- LfV Brandenburg
- LfV Berlin
- LfV Thüringer
- LfV Hessen
- IM/LfV Nordrhein-Westfalen (North Rhine–Westphalia)
- IM/LfV Rheinland-Pfalz (Rhineland-Palatinate)
- LfV Bayern (Bavaria)
- LfV Baden-Würtemberg
- LfV Saarland
- IM/LfV Schleswig-Holstein.

The organization has been successively restructured and streamlined to match both the threats viewed as important at the time and the agency's operational responsibilities. Currently, it is organized into the following divisions [known as *Abteilung* in German]:

- Z: administrative affairs
- IT: data processing and information technology
- 1: legal issues, data protection, VIP protection, liaison, observation, and intelligence
- 2: German right- and left-wing extremism and terrorism[23]
- 4: counterespionage, protective security, and countersabotage
- 5: activities posing a threat to security and extremist efforts of foreign nationals and from abroad, excluding Islamism
- 6: Islamist extremism and terrorism.

[23] Formed from the merger of the former Abteilungs 2 and 3.

Key Relationships with Other Intelligence and Law Enforcement Agencies

As previously noted, the BfV cooperates and works with a number of other German intelligence and policing bodies, including the following (see Thuillier, 2000, Annex 2):

- the Bundesnachrichtendienst [Federal Intelligence Service] (BND), which is responsible for intelligence on foreign states and international developments. This intelligence is the basis of a strengthened bi- and multi-lateral cooperation, makes suitable preventive strategies possible, and can help to defuse unfolding conflicts in time to ease them. As of this writing, the BND is relocating and moving many of its staff to its new headquarters in Berlin. However, about 1,500 of its staff are still based at its old headquarters in Pullach, just south of Munich.
- the MAD, which began as the Amt für Sicherheit der Bundeswehr [Office for Army Security] in 1956. The MAD is situated under the control of the Bundesminister der Verteidigung [federal minister of defense] and had a staff of 1,290 and a budget of €72 million in 2006. The organization also has eight regional offices across German territory and provides a counterintelligence and CT role similar to that of the BfV (but in the field of military security).
- the BKA, which is based in Wiesbaden but has a large satellite office at Meckenheim for close-in protection of diplomats. Unlike the various *Land* police, the BKA is a federal organization under the control of the BMI. It is responsible for police intelligence and coordination and federal-level investigations. Thus, while state police deal with normal criminal tasks, the BKA's key role is to counter international and domestic terrorism and organized crime (as defined in Sections 129a and 129b of the Strafgesetzbuch [Penal Code]). Consequently, the BKA was at the forefront of the struggle to counter the RAF and now works closely with the BfV and other intelligence organizations, providing them with operational support and executive powers of arrest in counterintelligence and CT scenarios and in cases of organized crime,

money laundering, forgery, and the large-scale trafficking of drugs.[24] These roles and powers are defined in the Bundeskriminalamtgesetz [Federal Criminal Police Office Law] promulgated in 1951.

- the BSI, which was formed by a December 17, 1990, law and is based at Bonn-Mehlem. The organization comprises technical and IT specialists who fulfill a number of tasks, including

> the evaluation of risks to security in the use of information systems by official organizations; the development of criteria for procedures and materials to test the security of information systems; the evaluation of the security of information systems and the awarding of security certificates; the obtaining of information materials and logistics destined to be used for classified information by official organizations or private bodies working under an official mandate; the application of techniques from different organizations in the selection of information materials; the application of technical security to police and the BfV IT in relation to terrorism and espionage. (Baud, 1998, p. 69, translated.)

Historically, as in many other countries, there was limited cooperation between the various federal intelligence and policing bodies. Consequently, on June 27, 1973, a federal law imposed cooperation between the various German intelligence organizations, the BfV, the BND, and the MAD. Currently, the directors of the BfV, BKA, and BND (or their deputies) meet weekly to exchange and discuss information on intelligence and security developments.[25] In addition, the Arbeitsgemeinschaft für die Sicherheit der Wirtschaft [Working Group for the Security of the Economy], based in Bonn, acts as an interface between the intelligence services and national industry, thereby providing economic intelligence for Germany (see Thuillier, 2000).

During late 2004 and early 2005, in a move similar to those made in a number of other Western nations, the German authorities established a joint analysis and fusion center, the Gemeinsamen Ter-

[24] For details of BKA roles and history, see Stock and Herz, 2007.

[25] Details from an untitled BfV memo of December 2007.

rorismusabwehrzentrum [Joint Counterterrorism Center] (GTAZ) (see Dietl, Hirschmann, and Tophoven, 2006). Based in Berlin, the GTAZ comprises experts from about 40 organizations, including the BfV, the BKA, the BND, the MAD, the various LfVs and LKAs, the BGS (recently renamed the Bundespolizei [border police]), the Zollkriminalamtes [Customs Criminal Office], and various transport specialists who fall into both the intelligence and policing pillars. This structure is not under the control of either the BfV or the BKA and has been established specifically to coordinate the response to Islamist terrorism by sharing information and joint analysis, enhancing dialogue between the organizations represented, and optimizing communication and coordination.[26] A number of the *Länder* have established their own regional intelligence-fusion cells and a separate joint Internet center was recently established to share the burden of costs and staffing for Internet monitoring.[27] Due to Germany's historical legacy and strong emphasis on data protection and privacy, such measures have led to considerable controversy and to claims by various politicians that the BfV's monitoring of the Internet and individuals' emails is illegal, unconstitutional, and a breach of civil liberties (see "German Intelligence Must Stop Computer Spying," 2007).

The BfV also regularly cooperates and exchanges information with other German federal and *Land* intelligence and policing organizations and its European counterparts, such as the UK's MI5 and France's DST. It first became active in coordinating and facilitating cooperation among international intelligence organizations through TREVI (which stands for Terrorism, Radicalism, Extremism, Violence Internationale), a structure created in 1976 to bring together intelligence and policing organizations from European countries affected by terrorism. (TREVI has been subsumed into the Justice and Home Affairs pillar of the European Union.) Germany's participation in such structures continues today with its engagement in the Kilowatt Group and the Club de Berne.[28]

---

[26] Author interview October 2007 with senior BfV intelligence officials.

[27] Author interview with senior BfV intelligence officials, October 2007.

[28] See Baud, 2005.

Oversight

As with other German intelligence organizations, oversight of the BfV occurs through a number of different controls, many of them parliamentary. The national coordinator for intelligence, who is currently the Bundeskanzlerin [federal chancellor] is not only charged with oversight and coordination between the various intelligence organizations but is also responsible for arranging meetings between the BfV (and other intelligence organizations) and the Parlamentarische Kontrollgremium [Parliamentary Standing Committee for the Intelligence Services] (PKGr), formerly known as the Parlamentarische Kontrollkommission [Parliamentary Control Commission]. The PKGr consists of nine members elected from the Bundestag and currently includes one member each from the left-wing PDS and the Green Party. PKGr members normally meet approximately once a month and are briefed by directors or very senior officials from the various intelligence organizations on current topics and operations. They have access to files and can task experts, such as former judges, to investigate specific cases of interest or concern. However, they are denied access to highly sensitive information, particularly to protect sources.[29] The framework for the PKGr's oversight of the various German intelligence organizations, including the BfV, was established in the federal Parlamentarische Kontrollkommission Gesetz [parliamentary control commission law] of April 11, 1978, and renewed by the federal law of May 27, 1992, following German reunification (see Thuillier, 2000).

The PKGr appoints four officials—sometimes current or former members of Parliament, judges, lawyers, or professors—to the G-10 Commission. This commission is responsible for oversight, control, and, ultimately, the authorization of the use of covert intelligence gathering by telephone, postal and technical intercepts, and covert searches. In extreme emergency situations, the BMI can authorize the use of covert intelligence-gathering methods, but the authorization will be retrospectively referred back to the G-10 Commission at a later stage.

[29] Author interview with senior BfV intelligence officials, October 2007.

The BMI briefs the commission monthly or before operations become effective.[30]

There are also more-general levels of parliamentary oversight, such as parliamentary questions and debates within the Bundestag and reports to the various Bundestag committees. In particular, there is regular oversight from the Innenausschuss [Interior Committee] and the Haushaltsausschuss [Budget Committee], but due to the sensitivity of details about specific funding for domestic intelligence operations, the latter committee often meets in a closed forum (see BfV, 2000). Some oversight is also exercised over the BfV by special committees of inquiry established by the Bundestag to examine particular intelligence-related matters, such as a recent inquiry into the use of extraordinary rendition on German soil.[31]

Finally, every German citizen is entitled to request that the BfW divulge whatever details the agency has recorded about him or her. The BfV will supply such information but will not release sensitive material, particularly if doing so might identify classified information about ongoing operational or methodological techniques, agents, or sources. A number of cases that have challenged this limitation in court have proved particularly difficult when they involve members of the extreme-left-wing PDS, which, although it is a monitored political party, has members in the Bundestag.

Problems or Controversies

Tension between members of the BfV and the BMI has existed over the best means of maintaining internal security and gathering domestic intelligence in Germany, particularly in relation to the level of openness required and processes related to the disclosure of information. This tension may be due, in part, to the fact that the BMI is responsible for the management of policing and domestic intelligence orga-

[30] Author interview with senior BfV intelligence officials, October 2007.

[31] Author interview with senior BfV intelligence officials, October 2007.

nizations in Germany. The two responsibilities have been traditionally separated and firewalled by the policy of *Trennungsgebot.*

Allegations continue to persist that, during the 1970s, 1980s, and early 1990s, in countering the extreme-left terrorist groups previously mentioned, the BfV resorted to a *schmutzigen Krieg* [dirty war] involving various excessive measures that breached human rights (see Todd and Bloch, 2003, pp. 125–127). One particular case that continues to remain controversial was the shooting of RAF member Wolfgang Grams and the arrest of Birgit Hogefeld in the Bad Kleinen railway station during an unsuccessful, source-led arrest attempt in 1993.[32] The GSG 9 officers involved claim that Grams was shot in self-defense after he drew a gun and killed their fellow officer Michael Newrzella, but some witnesses contend that Grams was deliberately shot while wounded (see Jackson, 1993). The resulting public outcry led to the resignation of the federal minister of the interior, Rudolf Seiters, and the dismissal of the federal prosecutor, Alexander von Stahl. Apart from these allegations and the ensuing resignations, the main damage was the exposure of the key BfV source for the operation, who was highly placed in the RAF. It was revealed that "Klaus Steinmetz had been active in various sections of the extreme left for a long time and had worked for the *Verfassungsschutz* [Protection of the Constitution, an abbreviated name for the BfV] for nine years" (Rojahn, 1998, p. 18). Despite attempts to conceal his presence at the time of the incident, he later had to be removed and placed in a witness-protection program.

Before unification, the BfV was the object of several high-profile infiltrations by the HVA, which made gaining the trust of other Western intelligence organizations difficult. One of the best-known examples of such infiltration was the defection of the BfV's first head, Otto John (who ran the organization from 1950 until his defection), to East Germany on July 27, 1954. Following the reunification of Germany, he was arrested and imprisoned and never granted pardon. More recently, Hansjoachim Tiedge, head of the BfV's counterespionage section, defected to East Germany on August 18, 1985. It was later discovered that, following the death of his wife and the emergence of

[32] For a detailed report, see Peters, 2004, Chapter 66.

alcohol-related problems, he had worked for the MfS for purely financial gain.[33] As a result of his betrayal, the MfS arrested 768 West German agents between June 1984 and August 1985 (see Baud, 1998).

Unlike some countries, and despite the prominence of data protection as a national issue, Germany has historically relied on data processing, data mining, and the use of profiling to identify potential terrorists or their support elements. Consequently,

> shortly after 9/11, German authorities conducted a computer-aided search of the type that had proven successful in profiling and eventually dismantling the Red Army Faction in the 1990s. Reportedly, this effort uncovered a number of radical Islamic "sleepers" in Germany, and a "considerable number of investigations have been started." (Miko and Froehlich, 2004, p. 9.)

As a result, the German authorities have established a central database to collect and store all information concerning Islamist extremists and violent jihadists. This has caused concern among civil libertarians and elements within the wider Muslim community because it raises issues of data protection and possible discrimination.

To counteract mistrust from left-wing and ecological political groups, the Green Party called in its 1998 electoral program for the dissolution of the various German intelligence services. Despite the current threat posed by Islamist terrorism and the important role played by such intelligence organizations in countering this threat, a small minority of individuals and politicians continue to call for such dissolution. Some members of the German public still view the various German intelligence and security services, including the BfV, negatively despite the strict parliamentary oversight and legal controls and the constitutional principle of *Trennungsgebot*. This perception may be, in part, the result of the legacy of such groups as the infamous Gestapo and the East German Stasi. Unfortunately, this legacy means that the BfV and other German intelligence services remain intrinsically mistrusted by many (see Thuillier, 2000).

---

[33] Author interview with senior BfV intelligence officials, October 2007.

Conclusion

Germany has developed a unique domestic intelligence structure based on numerous independent intelligence agencies reflecting the 16 *Länder*. This system, with its decentralization of responsibility to the *Land* level, was a deliberate historical anomaly instituted after the Nazi regime to ensure that excessive powers were not centralized in the hands of the federal government. Based in the policy of *Trennungsgebot*, this legislatively enforced decentralization of domestic intelligence, law enforcement, and other governmental structures ensured the dispersal of power and initially protected the fledgling democracy. However, there are concerns that the structure's raison d'être is no longer valid and may be affecting operational effectiveness. For example, the decentralized nature of this structure might obstruct federal operational coordination at the strategic levels, particularly during a time of heightened security or following a major terrorist incident. Such concerns have been highlighted by the experiences of the United States, the UK, and Spain, where major terrorist attacks have demonstrated the problems and obstacles associated with interorganizational cooperation and coordination. Perhaps one of the most significant concerns is that, despite the existence of NADIS, the BfV/LfV structure's decentralization and its associated legislation inhibit the flow of information and intelligence, negatively affecting timeliness and dissemination and, in the worst case, potentially allowing a piece of critical intelligence to fall through the cracks.

The structural replication inherent in the German domestic intelligence system leads to duplication and cost implications, but the old debate about the benefits of centralization versus those of local knowledge remains. The decentralized nature of the German domestic intelligence structure may be better suited than a centralized system to developing and exploiting intelligence due to its ability to take advantage of local knowledge and expertise, build better liaisons with local law enforcement officials, and better understand the local community and minority or other groups within it.

CHAPTER SIX

The United Kingdom

Lindsay Clutterbuck

Throughout the long history of the development of a UK CT intelligence capability, there has never been, apart from the two World Wars, a more intense, dynamic, and challenging era than the current one. The end of the Cold War had a profound effect on the UK intelligence agencies and, in particular, on MI5. Substantial changes to the service's role and the way it did business were already under way by 9/11, but in the aftermath of those attacks, the changes have been of a greater magnitude and are far more profound than anyone could have predicted.

These changes are being made across the board and are not concentrated just on MI5 or on all the intelligence agencies and the police. They go to the heart of the machinery of government that has been in place in the UK for decades. Foremost among the changes was the May 2007 removal from the Home Office of a range of criminal justice–related responsibilities and their transfer to the new Ministry of Justice. Consequently, the restructured Home Office is now more focused than before on its core functions of policing, intelligence gathering, CT, and preventing and controlling crime, immigration, and asylum. A new department, the Office for Security and Counter-Terrorism (OSCT), oversees these functions. In many respects, the Home Office is now more akin to a "Ministry of the Interior" along continental European lines. Its key role as the lead government department on CT in the UK is emphasized by the fact that the head of the OSCT is now a civil servant at the director-general level; the rank of the Security, Intelligence, and Resilience Coordinator in the Cabinet Office has been downgraded to below that of permanent secretary (Gregory, 2007).

At the same time, the structure for the delivery of CT policy and strategy has also changed. At ministerial level, the new Ministerial Committee on Security and Counter Terrorism has been established to oversee the work of the OSCT. The Prime Minister chairs a new National Security Committee, which meets monthly. In addition, a weekly security briefing, chaired by the home secretary, has been initiated (Gregory, 2007). One of the National Security Committee's first decisions was to recommend the publication of "a national security strategy . . . [that] will be published and presented in the autumn to Parliament for debate and decision in [the] House" (Brown, 2007). All these developments and their concomitant effects form the backdrop to this case study. It may be some time before their full impact and effectiveness can be assessed.[1]

The importance of these and other developments to the UK CT model cannot be overemphasized. The reason is that, contrary to popular belief, MI5 is not the only UK organization concerned with gathering, analyzing, and assessing intelligence relating to the terrorist threat to the UK, although it is the primary such organization. Equally important is the fact that the police do not just become involved when arrests must be made. The UK CT response is, like the threat that it faces, complex and dynamic. Independent yet interrelated organizations, structures, and systems are active participants. Each has its own specific roles and responsibilities, and it is their working relationships with MI5 that enable MI5 to fulfill its national security responsibilities.

Creation and Relevant History

The gathering of intelligence on potential threats against the internal security of the UK and the use of this intelligence to preempt attacks has a long and complex history. As an island nation, the UK's efforts are also interwoven, to a greater or lesser degree, with threats to the UK that originate from overseas. The first systematic approaches to carrying out this function were instituted during the Elizabethan period in

[1] For a full account of the changes to the Home Office, see Cabinet Office, 2007.

1570 and were undertaken and controlled for more than 30 years by a number of principal secretaries at the Court of Queen Elizabeth I. The most prominent of these secretaries were Sir William Cecil and Sir Francis Walsingham, who, as part of their duty to protect the Queen and the throne and defend the interests of the state against plots instigated by hostile countries and monarchs, ran spies and "intelligencers" in the UK and on the continent (Haynes, 1992).

It was not until after the 1829 formation of the Metropolitan Police Force in London, the first organized, uniformed police force on the British mainland, that the concept of gathering intelligence as a means to prevent crime, including public disorder and potentially revolutionary activities, became a function of a specific organization.[2] Beginning in 1832 at the latest, the Metropolitan Police Force deployed a small number of its officers in plain clothes to act against crime and criminals and gather intelligence related to potential public disorder. These activities came to light in 1833, when members of the National Political Union of the Working Classes exposed William Popay, a sergeant in the service.

With the full knowledge of the home secretary and on the orders of the commissioner of the Metropolitan Police, Popay had regularly attended meetings of the National Political Union of the Working Classes and other groups that were suspected of harboring revolutionary ideals and fomenting disorder at public marches and demonstrations (HMSO, 1833). The unfortunate Popay was dismissed for exceeding his orders but the committee upheld the general principle of using police officers to gather intelligence "for the preservation of the peace [and] the prevention of crimes" (Metropolitan Police Act of

---

[2] The first words of the first police instruction book emphasized the objective of prevention, although, for several years, prevention was seen as the role of uniformed police officers solely acting as a deterrent to crime by their visible presence:

> It should be understood at the outset that the principal object to be obtained is the prevention of crime. To this end every effort of the Police is to be directed. The security of person and property, the preservation of public tranquillity and all other objects of a Police establishment will thus be better effected than by the detection and punishment of the offender after he has succeeded in committing crime. (Metropolitan Police Service, p. 1.)

1829, 10 Geo. 4, c. 44). The principle was once more put into practice against a different potential threat in 1848 (Clutterbuck, 2006). Revolutionary upheavals racked Europe, and political refugees from many countries began to arrive in the UK. By the early 1850s, a regular flow of reports sent by the Metropolitan Police to the government was established to describe the activities (mainly fiery rhetoric) of refugees from Germany, France, Italy, and Poland. Despite the use of specific officers dedicated to this task, no formal unit existed in the Metropolitan Police to undertake this type of work in a systematic way until the establishment of Special Branch in February 1887.

Special Branch evolved in 1883 from a squad of officers located within the Criminal Investigation Department (CID) of the Metropolitan Police to deal with the campaign of bomb attacks that was being waged in the name of Irish republicanism by Irish Americans on the streets of London, Liverpool, and Glasgow. The home secretary set up the civilian Central Bureau of Intelligence to assist the squad and the scene was set for a turbulent period of mistrust, misunderstanding, and mutual dislike between their respective heads, Assistant Commissioner James Monro of Special Branch and Edward Jenkinson of the Central Bureau of Intelligence, a British civil servant who had been responsible for Fenian matters in Dublin. The upshot was that Jenkinson was eventually dismissed and his organization severely curtailed and Special Branch was given sole national responsibility for dealing with Irish republican terrorism and monitoring the activities of "Anarchists, Nihilists, Fenians, Clan na Gael-ites and other revolutionaries" (Sweeney, 1904, p. 34).

In the early years of the new century, it was clear that Germany was mounting a sustained campaign of espionage in Britain that was aimed primarily at military targets and designed to gather information to assist in planning an invasion. As a consequence, the existing arrangements in the police and the UK War Department were reviewed and, in 1909, the Secret Service Bureau, which later became known as the Security Service or MI5, was formed specifically to counter the threat from foreign (predominantly German) espionage in the UK (Porter, 1987, p. 167). The organization was established under military auspices and its first head, Captain Vernon Kell, had as his deputy a

retired former head of Special Branch, William Melville. The outbreak of war in 1914 led to a massive increase in the Secret Service Bureau's workload and an increase in its staff from 14 employees in July 1914 to 844 by November 1918 (Porter, 1987, p. 179).

After the war, the Security Service continued to function alongside the police special branches (each force was responsible for establishing and maintaining its own special branch). By 1945, the government defined its role solely as the "defence of the realm," particularly from subversion, defined as "the overthrow of the Government by unlawful means" (Stewart, 1945, p. 77, ¶37).

In 1952, following the change in ministerial responsibility for the Security Service from the prime minister to the home secretary, Home Secretary Sir David Maxwell Fyfe restated that principle in a directive issued to the director general of the Security Service (Fyfe, 1952, p. 80). Lord Denning, a high court judge appointed in 1963 to look into the Profumo affair summarized the Security Service in a 1952 report, stating that the service was "not established by Statute or recognized by Common Law. [It has] no executive powers [and is] a relatively small professional organization charged with the task of countering espionage, subversion and sabotage" (Fyfe, 1952, p. 91). He then delineated the way in which the Security Service and the police cooperated in that task:

> Those absences (they are not deficiencies)—the absence of powers and the absence of numbers—are made up for by the close cooperation of the Security Service and the police forces. In particular, in London, with the "Special Branch" of the Metropolitan Police and in the country, by the Chief Constables. If a search warrant is sought, it is granted to a constable. The police alone are entrusted with executive power. (Fyfe, 1952, p. 91)

The long-standing relationship between the police special branches and the Security Service was maintained in a low-key and generally effective way and the service dealt predominantly with subversion and its impact on public order and cases of espionage that typically involved the Soviet bloc. This role continued until the rise of terrorism in approximately 1969. At that time, terrorism began to manifest itself in the

UK in three ways: (1) as international terrorism, in which individuals from a variety of organizations, predominantly from the Middle East, carried out attacks in London; (2) as Irish republican and Loyalist terrorism both in Northern Ireland and on the British mainland (where the first attack occurred in 1973); and (3) as domestic terrorism, perpetrated by the Angry Brigade and their anarchistic imitators.

Due to the need to gather intelligence on foreign nationals operating in the UK as members of terrorist organizations based abroad, the Security Service had to work closely with the other intelligence agencies whose responsibilities also involved intelligence gathering. These agencies were predominantly the Secret Intelligence Service (SIS), responsible for intelligence gathering outside the UK, and the Government Communications Headquarters (GCHQ), responsible for gathering intelligence from electronic communications. Over time, the Security Service became the lead agency against all such terrorist threats. However, the responsibility for intelligence gathering (and its exploitation) against Irish republican terrorists remained in the hands of the police. In Northern Ireland, the Special Branch of the Royal Ulster Constabulary took the lead, and, on the British mainland, the Special Branch of the Metropolitan Police did so, assisted by the special branch of each police service.

The first step taken to recalibrate the situation was the passage of the Security Service Act 1989, which was made possible primarily by the end of the Cold War and the dramatic lowering of the potential threat to the UK from Soviet Bloc espionage and subversion. For the first time in its history, the existence of the Security Service was officially acknowledged and its responsibilities were made public. The second step came in 1992, when lead responsibility for intelligence gathering against Irish republican terrorism on the British mainland was transferred from the Metropolitan Police Special Branch to the Security Service ("Counter-Terrorism," 1992, cc. 297–299). The process was completed in 2006 when Security Service also assumed the lead role in Northern Ireland itself ("'No Need,'" 2006). All aspects of UK intelligence gathering in the context of both international and Irish

republican–related terrorism were thus lodged in the Security Service.[3] In 1996, the Security Service Act was amended to give the Security Service the power to act "in support of the prevention and detection of serious crime" at the behest of the police or other law enforcement agency (Security Service Act, 1996). Ironically, as the implications for the Security Service of assuming responsibility for intelligence work against Irish republican terrorism on the British mainland began to unfold, the Irish Republican Army (IRA) was already beginning to abandon terrorism. Its last known attack in Britain occurred in 1997 and was followed during the next five years by several attacks mounted by splinter groups, such as the Real IRA and the Continuity IRA.

It was neither the IRA nor the end of the Cold War that brought about the most dramatic change in the Security Service. It was the events of 9/11 in the United States and the attacks that quickly followed in the UK and elsewhere around the globe. The main consequence of these attacks was a refocusing of Security Service intelligence priorities to counter the threat from al Qaeda and the violent ideology it and its adherents espouse. It is not only the intelligence focus that has changed, however: The scale and scope of Security Service activities that support this focus have also expanded substantially. By 2008, the service's staff almost doubled in size (Brown, 2006) and the organization established regional offices in population centers other than London (Norton-Taylor, 2005). As the Security Service reaches its 100th anniversary and establishes these offices, it will have—for the first time in its long history—a nationwide presence to carry out its national responsibilities.

Mission and Critical Capabilities

Until the Security Service was put on a statutory footing under the Security Service Act 1989, the UK government had not officially acknowledged its existence; hence; the first words of the act are "There

[3] Extremism linked to animal rights remains a police responsibility.

shall continue to be a Security Service" (Security Service Act 1989, §1[1]). The act then defines the service's role and responsibilities:

> The function of the Service shall be the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means. It shall also be the function of the Service to safeguard the economic well-being of the UK against threats posed by the actions or intentions of persons outside the UK. (Security Service Act 1989, §§ 1[2], 1[3].)

Since its passage, the Security Service Act has been amended by five separate acts. The most important of these was the Human Rights Act 1998 that incorporated the provisions of the European Convention on Human Rights into UK law (HMSO, 2006, p. 4).

It is important to note that the Security Service does not confine its activities to gathering intelligence to counter terrorist activity. It actively investigates, assesses, and exploits intelligence in a variety of areas and does so in active cooperation with other members of the UK intelligence community and with law enforcement organizations, such as the police, Her Majesty's Revenue and Customs (HMRC), and the immigration authorities. Similarly, not all its resources are dedicated solely to CT efforts. The service's traditional role against espionage and foreign-state activity now also includes the responsibility to

> frustrate procurement by proliferating countries of material, technology or expertise relating to weapons of mass destruction; watching out for new threats or re-emerging types of threat; protecting Government's sensitive information and assets, and the Critical National Infrastructure (CNI), and assisting the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ) in the discharge of their statutory functions. (MI5, undated [a].)

To counter threats to national security, the service works closely with others to "investigate, act, advise and assist" (MI5, undated [a]). It

does so by obtaining secret intelligence, analyzing and assessing it, and then deciding on counteraction and protective measures.

Priorities within the service are set according to the national intelligence requirements as drawn up by the Joint Intelligence Committee and endorsed by government ministers. The principal techniques used by the service in carrying out intelligence investigations are the use of

- covert HUMINT sources (CHIS) (i.e., agents who can provide secret reporting on a target under investigation)
- directed surveillance (i.e., following and observing suspects)
- interception of communications (i.e., telephone calls, emails, and letters)
- intrusive surveillance (i.e., eavesdropping operations).

The authorization and use of all of these techniques are subject to the provisions of the Regulation of Investigatory Powers Act 2000 (RIPA). The most intrusive techniques require personal authorization by a secretary of state, usually the home secretary. When applying for a warrant to carry out these activities, the service must demonstrate that what it proposes to do is both necessary for the protection of national security and proportionate to what it seeks to achieve. A final test is that the information that the service hopes to obtain could not reasonably be obtained by other means. Only when Home Office officials are satisfied that these criteria have been fully met and the case is a strong one is the application placed before the secretary of state (MI5, undated[b]).

The powers that the Security Service can exercise under RIPA are not unique. They are also available to a wide variety of government agencies, although the Security Service and the police are part of a much smaller group that can apply for authority to deploy all of them (see Table 6.1).

The "Oversight and Accountability" section of this chapter further explores issues of external oversight of the use of these powers in operational deployments and the Security Service's accountability for their use.

Table 6.1
Powers and Numbers of Authorized Agencies Under RIPA, Including the Security Service

Powers Under RIPA 2000	Authorized Agencies
Deployment of directed surveillance	59
Deployment of intrusive surveillance	15
Interference with property or wireless telegraphy and entry onto land	10
Covert investigation of computers	
Via interference with property	10
Via intrusive surveillance	13
Via directed surveillance	59
Examination of mobile phones	10
Investigation of communication data	7[a]
Interception of communications	11
Deployment of CHIS	36

SOURCE: Harfield and Harfield, 2005, cited in Gregory, 2008.

[a] The government has proposed new statutory arrangements to replace existing voluntary ones. Under the proposed arrangements, 659 government agencies will be able to apply to receive communication data. There will be three levels: subscriber only, subscriber and numbers dialed, and previous numbers dialed plus phone location. Only the police and the Security Service can apply for the last level (McNulty, 2007).

Leadership and Human Capital

A director general (DG) heads the Security Service and is accountable to the home secretary for the Security Service's operations and activities. In turn, the home secretary is accountable to the prime minister for the Security Service, as it is the prime minister who bears ultimate responsibility for national security. Both the home secretary and the prime minister are individually accountable to Parliament. In consultation with the home secretary, the DG draws up an annual public-

service agreement, which includes agreed priorities for resource allocation. Despite this role, however, the home secretary has no power to issue orders to the DG because the DG is a Crown servant, not a member of the civil service. As a consequence of these arrangements, the incumbent occupies a unique position among all other heads of government institutions: The DG and the heads of the other intelligence agencies have the right of direct access to the prime minister.

The words of Sir Findlater Stewart on the Security Service's role are still an accurate summation of the DG's role and the kind of individual that is required to undertake it:

> That appointment is one of great responsibility, calling for unusual experience and a rare combination of qualities; but having got the right man there is no alternative to giving him the widest discretion in the means he uses and the direction in which he applies them. (Stewart, 1945 report, p. 79.)

The most significant change to this assessment has been the appointment in the past 15 years of two female DGs, Dame Stella Rimington (served 1992–1996), who was also the first DG to be publicly named as such by the government, and Dame Eliza Manningham-Buller (served 2002–2007). The current DG is Jonathan Evans, a career Security Service officer who, before his appointment, served as deputy DG to Dame Eliza.

There have been 15 heads of the Security Service since it was first established under Captain (later Major General) Sir Vernon Kell in 1909, who served as the service's head for 31 years. The career path of a potential DG, which began to take on its current form in the mid-1980s, is that DGs are selected from inside the service, have served as deputy DG under the previous DG, and serve as DG for about five years. This pattern now appears to be well established, and, when the time comes to consider appointing a new DG, many feel that only compelling reasons could justify a departure from that pattern.[4] However, there is another perspective: The DG should be a professional

[4] Interview with a retired senior Home Office official, 2007.

appointment and not a political one, but it is not a necessity that the candidate be appointed from inside the service. In this view, a wide range of suitable candidates should be considered to stop any closed-shop insularity from developing.[5]

In terms of overall staffing numbers, the Security Service has traditionally been small. During 1993, a year after it had taken over the lead for Irish republican terrorism on the British mainland, it had approximately 2,000 staff, just over half of whom were women and just over half of whom were younger than 40 (MI5, 1993, p. 9). A gentle decline in the number of staff ensued, with the total in 1998 falling to about 1,900 plus 100 on attachment or secondment (MI5 and Central Office of Information, 1998, p. 28). The period immediately before 9/11 saw a further drop to about 1,800 staff in June 2001 (Lander, 2001). Immediately after 9/11, the downward trend was brought to a halt and, by 2003, the total had increased back to its 1993 level of 2,000 (Manningham-Buller, 2003). In 2004, a decision was made to expand the service to deal with the burgeoning threat; as of October 2007, the organization had a staff of approximately 3,000. Of these, 44 percent are women and 54 percent are under the age of 40 (MI5, undated[a]). By 2008, under current plans and resource allocation levels, the service will have almost doubled in size from its 2001 nadir to a staff of about 3,500 (Brown, 2006). The ultimate objective is to have a staff of 4,000 by 2011, with 25 percent working away from London in the eight new regional offices (Evans, 2007c).

Management and Process

The detailed tasking and resourcing processes in the intelligence agencies are not a matter of public record, so detailed information is difficult to come by. It is more readily available concerning the police role in CT, but the difficulty here is the lack of clarity in the roles of

[5] Interview with a retired senior intelligence official, 2007.

police units from force to force.[6] However, a general overview can be obtained.

The Security Service investigates areas of concern that the home secretary validates and that have been subject to parliamentary scrutiny. Its investigative work and its own assessment of how to meet its requirements drive its day-to-day operational activity. Priorities are adjusted "according to the national requirements for intelligence, set by the Government, drawn up by the Joint Intelligence Committee and endorsed by Ministers" (MI5, undated[c]). In turn, the Security Service communicates to the police (and other organizations) the intelligence requirements that are most relevant to the nature of their work and details those aspects in which the service is particularly interested. The difficulty for the police is that there are a wide variety of requirements, some of which may concern only one force or a small number of forces, thus making the production of a suitable, single, national requirement document a challenge.[7]

Organizational Structure and Funding Patterns

In addition to the Security Service itself, two semiautonomous organizations are responsible for carrying out different aspects of the wider service role in protecting national security. They are the Joint Terrorism Analysis Centre (JTAC) and the Centre for the Protection of National Infrastructure (CPNI), both of which are collocated with the Security Service. JTAC was established as an autonomous organization in June 2003 as the UK center for the analysis and assessment of the threat from international terrorism (MI5, undated[d]). Representatives from 11 government departments, the police, and other organizations work in JTAC to analyze all relevant intelligence from the UK and overseas, set the national threat level, and produce in-depth reports on terrorism trends, organizations, and capabilities. The head of JTAC is accountable to the Security Service DG, and JTAC staff work especially closely

6 Interview with a senior police officer, 2007.

7 Interview with a senior police officer, 2007.

with the Security Service's International Counter Terrorism, Counter Espionage and Counter Proliferation branch.

The CPNI, formed on February 1, 2007, from the merger of two preexisting organizations, is an even more recent innovation.[8] Its role is to protect national security through the provision of expert advice on all aspects of security to businesses and organizations that together comprise the critical national infrastructure and other vital elements. Like JTAC, CPNI is an interdepartmental organization with representatives from the Security Service, the Communications Electronics Security Group (an element of GCHQ), police, and others. The head of CPNI is accountable to the Security Service DG.

Until recently, government funding for all the intelligence agencies was paid from the same source: a single sum of money known as the Single Intelligence Vote, which is determined annually by ministers and to which Parliament agrees (M15 and Central Office of Information, 1998, p. 34). In 1998, the Security Service budget was "less than £140 million" out of £701 million (M15 and Central Office of Information, 1998, p. 34). In October 2007, following a wide restructuring of the UK CT response, a new Single Security and Intelligence Budget was created to "bring together all dedicated counter-terrorism and intelligence funding for the Security and Intelligence Agencies, the police and all parts of government responsible for addressing the threat from terrorism" ("Security and Intelligence 2007 Pre-Budget Report," 2007). The Ministerial Committee on National Security, International Relations and Development, chaired by the prime minister, will annually review the spending plans under this budget.

The Single Security and Intelligence Budget is set to rise to £3.5 billion by 2010–2011, "more than triple the pre 9/11 levels" ("Security and Intelligence 2007 Pre-Budget Report," 2007). Traditionally, the breakdown of the figure into the division of funding for the three agencies is not made public for security reasons (Security Service, undated[a]), but a substantial element of the Security Service assignment will likely be

[8] They were the National Infrastructure Security Co-Ordination Centre and the National Security Advice Centre (see CPNI, undated).

used to meet the agency's objective of doubling its 2001 staff levels and further consolidating and operating its eight new regional offices.

The Security Service is required to operate within the financial framework of government accounting, so it is subject to audit by the National Audit Office (NAO). That office has full access to the service's accounts so that it can carry out its role.

Security Service priorities—and, therefore, its resource allocation—have changed over the past fifteen years. In 1993, 70 percent of the service's resources went to CT (44 percent to Irish republican–related and other domestic CT, 26 percent to international CT), 25 percent went to counterespionage and counterproliferation, and 5 percent went to countersubversion (MI5, 1993, p. 12). Today, CT accounts for 80 percent of the service's resources (17 percent goes to Irish republican–related and other domestic CT, 63 percent to international CT), 5 percent goes to counterespionage, and 2 percent to counterproliferation. Emerging and other threats account for 0.5 percent of the resources and external assistance to SIS and GCHQ accounts for 3 percent. Protective security (i.e., measures focused on protecting government-classified assets and CNI) also accounts for 9 percent of resources. The service is no longer active in the field of subversion and it suspended activity relating to serious and organized crime in early 2006 to concentrate on CT (MI5, undated[a]).

Key Relationships with Other Intelligence and Law Enforcement Agencies

Responsibility for the UK national intelligence function is divided among three dedicated intelligence agencies. They are the Security Service (which focuses on national security threats to the UK, including their overseas dimension), SIS (which conducts intelligence gathering outside the UK that is related to national security and the economic well-being of the country or supports the prevention or detection of serious crime), and GCHQ (which focuses on intelligence derived from

electronic communications).[9] The Security Service works closely with SIS and GCHQ and, when required, with national law enforcement organizations (e.g., the Serious Organised Crime Agency [SOCA] and HMRC).

To fulfill its national remit and to contribute to the many other aspects of CT, the Security Service must also function at the regional and local levels. Consequently, it works closely not only with police forces at a combined, national level but also with individual, local police forces (43 in England and Wales, eight in Scotland, and one in Northern Ireland). Historically, the point of liaison and the level at which the service has formed close working relationships on all relevant issues has been the special branch of each force. A set of ministerial guidelines provides the parameters within which each special branch is expected to operate, although implementation is left to each chief constable (Home Office, Scottish Executive, and Northern Ireland Office, 2004). The primary function of a special branch is to carry out "covert intelligence work in relation to national security"; thus, each special branch assists the Security Service in "carrying out its statutory duties under the Security Service Act 1989 [and] also supports the work of the Secret Intelligence Service" (Home Office, Scottish Executive, and Northern Ireland Office, 2004, p. 7). Since 9/11, the systems and structures that had evolved over many years to enable the police and the Security Service to work together against threats from Irish republican and Loyalist terrorism, international terrorism, and domestic extremism have undergone substantial change. This change has been driven predominantly by a steep decline in the threat from Irish republican terrorism and a substantial increase in the threat from terrorist activity linked to the violent jihadist ideology typified by al Qaeda. Since 2004, a trend has become discernible in these types of groups and networks. Their activities involve "groups of British citizens traveling to Pakistan to receive training and instructions, then returning to the UK and building up their networks [there, then] moving towards launching attacks" (Clarke, 2007). In December 2008, Prime

[9] As had occurred with the Security Service in 1989, the Intelligence Services Act 1994 placed both SIS and GCHQ on a statutory footing (see §§ 1 and 3, respectively).

Minister Gordon Brown stated that "three quarters of the most serious plots investigated by the British authorities have links to al Qaeda in Pakistan" (Hinsliff, 2008).

Consequently, the way in which intelligence is gathered, disseminated, and acted upon has been reconfigured in the past three years, and the changes are not yet complete. The most noticeable outcome of these changes is seen in the relationship between the 52 UK police forces and the Security Service. CT is a constant focus of all of the police services in the UK, as it was when the IRA was active, but the "map" of terrorism on the British mainland has now changed. To reflect this, the police service recently established Counter Terrorism Intelligence Units (CTIUs) at the regional level and proactive, investigative Counter Terrorism Units (CTUs).[10] Both work closely with the Security Service (as the force special branches continue to do) and the relationship is facilitated through the eight newly established Security Service regional offices. From a police perspective, the new structures "will definitely increase our ability to respond to the intelligence generated by the Security Service."[11] Now more than ever, the working relationship between the police and the Security Service in the area of CT is a joint partnership.

Police gather intelligence relevant to the Security Service at two levels: in police force areas and at the regional level. This intelligence-gathering effort is prioritized and directed by the force's or region's Tasking and Coordinating Group. The concept of police regions in which CT operational activities that span two or more force boundaries are coordinated and developed is embryonic. It is thus in this area that the Security Service, through its new regional offices, interacts with special branches to conduct intelligence-gathering and intelligence-development operations. Predetermined thresholds for the product ensure that as much work as possible happens at the local and regional

[10] Except for SOCA, there is no national police organization in the UK. The chief constable of each force bears sole constitutional responsibility for that force area. The new regional units are "owned" by the chief constable of the force in which they are located; they have a regional remit and are defined as police national assets (author interview with a senior police officer, 2007).

[11] Author interview with a senior police officer, 2007.

levels and that only material that may be relevant at the national level is sent on to the Security Service in London.[12]

A second, equally important change has been required in the key area of decisionmaking in relation to potential police executive action (i.e., the arrest of suspects). In the past, particularly when dealing with cases of IRA terrorism, intervention was heavily influenced by one factor: the sufficiency and quality of the evidence available. Under today's new, less certain, and potentially more lethal situation, a new concept of operations had to be formulated, and intervention is now driven by the risk to the public. If the risk to public safety is unacceptable, then intervention will occur regardless of the state of the evidence.[13]

The main consequence of this approach is that police detectives whose role is primarily to gather evidence become involved far earlier in investigations initiated by the service. Prior to this change, the investigations were intelligence based and frequently conducted in conjunction with the appropriate police special branch, whose remit is to gather and develop intelligence within its force area. Nowadays, the vast majority of police investigative activity takes place in this intelligence-development phase.[14] When it is determined that the intelligence-gathering investigation may require executive action, the multiagency Executive Liaison Group assumes strategic oversight of the case. The group is formed expressly for that purpose and consists of senior police detectives, senior special branch officers, and Security Service officers.

Oversight

Before 1952, the prime minister was directly responsible for security. Following a recommendation in a report by Sir Norman Brook, the responsibility was transferred to the home secretary because the Home

[12] Author interview with a senior police officer, 2007.

[13] Author interview with a senior police officer, 2007.

[14] Author interview with a senior police officer, 2007.

Office has "the ultimate constitutional responsibility for 'defending the realm' against subversive activities and for preserving law and order" (Brook, 1951, cited in Denning, 1992, p. 79). Brook recommended that the Security Service not be considered a department of the Home Office and that it operate independently under its own DG (Fyfe, 1952, p. 80). However, it was envisioned that the prime minister would still discuss with the DG

> from time to time . . . the general state of his work and particular matters that might be of specially close concern to him. And on matters of supreme importance and delicacy, the Head of the Service should always be able, at his initiation, to arrange a personal interview with the Prime Minister. (Brook, 1951, cited in Denning, 1992, p. 80.)

These arrangements, which still apply today, form the core of the political accountability that governs the Security Service.

A recent European Union report known as the Venice Commission identifies four methods by which states can ensure the accountability of their security and intelligence agencies: parliamentary, judicial, expert, and complaint mechanisms (Venice Commission, 2007, p. 17). The report, which examines the democratic oversight of security services, states that the UK's use of "serving or retired judges [sitting] on expert bodies . . . should be regarded as a form of expert rather than judicial control" (Venice Commission, 2007, p. 7). Therefore, in these terms, as the UK does not use intelligence agency–specific bodies of experts to provide oversight, it appears to use only two—parliamentary and complaint mechanisms—of the four possible oversight categories.

The real situation is more complex than this assessment suggests, however. For example, although the judiciary has no regular or routine involvement in formal oversight over the Security Service, the service would not be immune from court scrutiny in certain circumstances. Furthermore, retired and serving judges have a vital role to play in the oversight of the intelligence services in general because statute requires that these judges head a variety of so-called complaint mechanisms and because their role and remit within such mechanisms are more comprehensive and proactive than just investigating complaints.

A more useful categorization of the web of UK oversight bodies concerned with ensuring that the Security Service complies with its statutory duties and responsibilities is shown in Table 6.2 and discussed in subsequent sections.

Ministerial Oversight

The UK has two means of political oversight. The first is ministerial. As previously described, the Security Services Act 1989 gives the Security Service its statutory footing. Under this law, the service is placed under the authority of the home secretary, who is a senior minister. This minister is responsible directly to Parliament for the service's actions and activities. The act also requires that the Security Service DG report formally to the prime minister on an annual basis and stipulates that the prime minister is responsible to Parliament. Until the early 1990s, this was the only political oversight mechanism vis-à-vis the Security Service.

Parliamentary Oversight

In 1994, the Intelligence and Security Act established the parliamentary Intelligence and Security Committee (ISC). All its members are privy counsellors, its meetings are held in private, and its remit covers all the intelligence agencies. The committee reports annually to Par-

Table 6.2
Levels of Accountability for the Security Service

Category	Mechanism
Ministerial	The secretary of state for the Home Office
	The prime minister
Parliamentary	The ISC
Functional	The IPT
	The Intelligence Services commissioner
	The Interception of Communications commissioner
	The independent reviewer of terrorist legislation
	The NAO

liament and can investigate specific issues of particular concern. Its reports are publicly available (Cabinet Office, 2008). However, current arrangements are now under review, and, in July 2007, the prime minister announced that

> the Government is consulting on how in future the ISC should be appointed and should report to Parliament—with, where possible, hearings in public, a strengthened capacity for investigations, reports subject to more parliamentary debate and greater transparency over appointments to the committee. (Brown, 2007.)

Functional Oversight

RIPA (Part IV) established the Investigatory Powers Tribunal (IPT) and made it responsible for investigating any member of the public's complaints about any public authority's use of any of the powers provided under the act. IPT also conducts regular and systematic reviews of intelligence agencies' use of a variety of investigative techniques, such as "interception, property interference and covert investigative practices" (IPT, 2006). Both the president and vice president of the IPT "must hold or have held high judicial office" and are appointed, as are the other seven members, directly by the Queen. This system ensures that IPT members are independent of the government (IPT, 2006).

More specifically, the Intelligence Services commissioner oversees the intelligence agencies in general while the Interception of Communications commissioner oversees intelligence agency interception practices in particular. These commissioners are independent individuals who, like IPT members, "must hold or have held high judicial office" (HMSO, 2006, p. 4). They review the exercise of the powers that rest with the relevant secretary of state and certain categories of the intelligence agencies' activities (including those of the Security Service). They report directly to the prime minister on an annual basis, and unclassified versions of their reports are sent to Parliament.

A new and still-evolving oversight mechanism has come into existence in recent years due to the development of the concept of "control orders" under the Terrorism Act 2005. Control orders, which restrict the movement of suspected terrorists, are issued primarily on the basis

of intelligence when there is not sufficient evidence to charge an individual and put him or her on trial for terrorist activity. As of October 2007, control orders apply to 14 people in the UK (Dyer, 2007). Under the Terrorism Act 2000, an independent reviewer was appointed to oversee how the powers that act granted to the police were being used. This role was extended to cover the Terrorism Act 2005, and because control orders are underpinned by intelligence, the Security Service's acquisition and use of intelligence in these cases now come under the services' purview. A quarterly report is submitted to Parliament on its use in these cases.

The NAO oversees the finances and expenditures of the Security Service, the other intelligence agencies, and the police. The NAO is the wholly independent body that scrutinizes public spending on behalf of Parliament to ensure that monies are spent with economy, effectiveness, and efficiency (NAO, undated). The Intelligence Services Act 1994 and the Security Services Act 1989 both made provisions for the NAO to carry out its duty of scrutiny by giving it "full access to the agencies records," with certain restrictions (NAO, 2000). However, these arrangements prevent the NAO from divulging the information that it has obtained unless the government specifically lifts the restriction. In the past, the NAO has produced classified reports on the intelligence agencies' expenditures, particularly on the purchase, refurbishment, and fitting out of Security Service and SIS headquarters buildings in the early 1990s (NAO, 2000, p. 3). These reports were then brought to the attention of the chair of the Parliamentary Committee of Public Accounts and, some years later, declassified and put into the public domain (NAO, 2000).

Performance Metrics

There are no formal, published metrics to determine Security Service performance. Consequently, it is not possible to make comparative assessments of its overall quality. The public perception of the service's success or failings in countering terrorism is based almost entirely on media reporting. The media employ different sources to gather the

information they use in their reports. Foremost among these sources are relevant criminal trials. Strict sub judice rules before a trial begins and, if necessary, court-imposed reporting restrictions during the trial ensure that little information from the police or the Security Service reaches the public domain before or during trials. However, once this stage is passed, the media are free to focus on all the aspects of the case, including the services' role and actions.

Before 1992, the Security Service was able to operate with very little media scrutiny, so few facts informed or influenced public support for the service. However, once the Security Service took over as the lead agency on the British mainland for gathering intelligence on the IRA, this situation began to change. With each passing incident, arrest, trial, and conviction (or acquittal), the service and its successes (or perceived failures) began to be scrutinized publicly on a regular basis and, almost for the first time in the service's history, facts were available to inform judgments.

This type of scrutiny occurred during the April 30, 2007, convictions of five men who had planned and prepared to carry out bomb attacks in the UK. Details released about Operation Crevice gave a full account not only of the police's role in this investigation but also that of the Security Service ("Five Get Life over UK Bomb Plot," 2007). The court case revealed that two of the individuals who participated in the July 7, 2005, suicide attacks on the transport system in London were known to the Security Service before those attacks. They had met on four occasions in early 2004 with the leader of the Crevice group, Omar Khyam ("MI5 Followed UK Suicide Bomber," 2007). As a consequence of this revelation and the questions and comments in the media, the Security Service updated its Web site at the conclusion of the trial with the DG's statement on the verdict. It also provided its own account of the circumstances to answer the following question posed by the media: "If the Security Service and Police had already come across two of the bombers before 2005, why did they not prevent the attacks in London on 7th July?" (Evans, 2007a, 2007b).

Any overtly hostile act against a state and its citizens is seen as an intelligence agency failure. This is irrespective of the fact that no liberal democracy has, or is even likely to contemplate, the kind of intelli-

gence apparatus that would be necessary to make this a valid criticism. On the other hand, operational successes may need to remain unpublicized and hence unknown. A former Security Service DG, Dame Eliza Manningham-Buller, put it succinctly when she said, "it is something that we just have to put up with, that our failures are apparent to all, our successes usually known to a few. Like the best administration, you never notice it. It is only when things go wrong that you do" (Manningham-Buller, 2003).

Problems or Controversies

As well as being judged absolutely on operational success or failure, intelligence agencies are inherently prone to allegations that they have abused their powers. In the case of the Security Service, there have been few proven cases of deliberate abuse. In 2006, a Special Immigration Appeals Commission judge criticized the Home Office and the Security Service for submitting contradictory intelligence on two terrorism suspects to court hearings. The Home Office and the Security Service acknowledged that a procedural error had been made and accepted the commission's recommendations for ensuring that it would not occur again ("Judge Critical of MI5 Testimony," 2006).

A recurring allegation concerns one aspect of the Security Service's role in the late 1970s and early 1980s—namely, that of countering subversion. The service is accused of having been politicized at times and particularly during the 1980s, when MI5 conducted countersubversive operations against left-wing activists and organizations that Prime Minister Margaret Thatcher termed "the enemy within." These operations have subsequently been referred to as "MI5's past abuses" (Burch, 2007, pp. 7–8). However, this conflation of 1980s political rhetoric with the service's subsequent activities to protect the UK from actions "intended to overthrow or undermine Parliamentary democracy by political, industrial or violent means" does not appear to accurately depict the situation.[15]

[15] The definition of subversion in use at the time is found in MI5, 1993, p. 17.

Subversive groups and individuals were particularly active in the UK during the 1970s and 1980s, a period of industrial upheaval, civil strife, and public disorder.[16] Using conspiratorial methods and "entryist" tactics, "subversive groups sought to infiltrate and manipulate bona fide organisations, such as trades unions or pressure groups, as a way of exerting influence out of proportion to any support they could achieve through the ballot box" (Security Service, undated [e]). The Security Service's role was to investigate and counter this subversive element, not the organization or group in which that element was active. Prime Minister Gordon Brown's recent suggestion that the limit preventing classified official papers from entering the public domain for 30 years be reduced to 20 years could change perceptions of the service's operations during this period ("Secrets of the Thatcher Years May Be Revealed a Decade Early," 2007).

In the past five years, MI5 has found itself at the center of recurring allegations relating to its activities in Pakistan. On suspicion of terrorism, Pakistani authorities have arrested a number of suspects who either are UK citizens or hold dual UK/Pakistan citizenship. Some suspects have been extradited to the UK to stand trial or released without charge and returned. At least two of them have alleged that, while they were in custody in Pakistan, they were abused or tortured and later interviewed by unnamed representatives from the UK—whom they allege were from MI5 (Cobain, 2008a).

The inference now being drawn in some quarters is that MI5 outsourced the torture of suspects to the Pakistani authorities or was at least aware of it and took no steps to prevent it. MI5 countered the allegations, stating that the "Security and Intelligence Agencies do not participate in, solicit, encourage or condone the use of torture or inhumane or degrading treatment" (Cobain, 2008a). However, this denial was not sufficient to stop a member of Parliament from filing a formal IPT complaint on behalf of one of his constituents (Cobain, 2008b).

On a previous occasion, the ISC investigated a similar allegation and

---

[16] For background accounts, see Whitehead, 1985, and R. Clutterbuck, 1978. Rimington, 2001, describes MI5's role.

> gave the Security Service a clean bill of health in 2005 [and commented that] when Security Service personnel had come across instances when poor treatment of detainees was suspected [they] notified the detaining authorities immediately and this was followed up with an official complaint from London. (Cobain, 2008b.)

In terms of process and procedure, these new allegations break new ground by having the IPT carry out the investigation. It remains to be seen how the IPT will rise to this challenge and how much confidence is placed on its eventual findings.

Conclusion

The concept of the state gathering intelligence on its citizens and residents in order to "keep the Queens' Peace" and to act in "defence of the realm" is deeply embedded in the history of the UK. Throughout almost all of the 20th century, these functions were performed by the police or by the police with the Security Service and the other agencies. Throughout that period, there was a clear division between police and intelligence roles, although through their own special branches, the police have operated in close conjunction with the Security Service. For much of its history, the Security Service has been able to rely on a blanket of secrecy to keep its work out of the public eye. Since 1992, however, two factors have fundamentally altered the environment in which the service operates. The first of these was the transfer of the lead responsibility for intelligence gathering against Irish republican terrorism on the British mainland from Metropolitan Police Special Branch to the Security Service, thus giving the service unequivocal responsibility for all intelligence operations relating to all aspects of terrorism. The second was the rise of a new terrorist threat to the UK in the form of violent jihadism and extremism. These factors will ultimately ensure that the UK arrives at a new paradigm to protect its national security.

The threat today and the lead role that the Security Service has in countering it will ensure that the service is increasingly in the eye of the media and that public awareness of the organization will hence

increase. The service's involvement is now critical to the gathering of evidence in cases of terrorism that are brought before a court, and it is no longer possible to keep the service's role out of court proceedings.

Perhaps surprisingly, the Security Service is undergoing a transformation like that of the FBI in the United States. The FBI is a long-established organization with a primary focus on crime and criminal investigations and an important but secondary role to play in CT investigations. As a consequence of 9/11 and subsequent events, however, the FBI is now rebalancing its role and responsibilities and moving into CT intelligence operations on a much greater scale. Both organizations are having to move into new areas of operational responsibility.

For much of the 20th century, the Security Service was a long-standing domestic intelligence–gathering agency that, like the FBI, had an important but secondary role to play in police CT investigations. Today, the service's CT role in the criminal-justice system has expanded enormously due to the increased numbers of investigations into terrorism suspects whom police subsequently arrest and thus later appear in court. Consequently, the Security Service is, like the FBI, also having to rebalance its role and responsibilities. As in the FBI, this rebalancing process is occurring simultaneously with substantial increases in workload, substantial increases in the complexity of the international investigatory environment, and an unprecedented influx of new staff drawn from secondments and recruiting.

It may not be too great a stretch of the imagination to look to the future and see a time when the Security Service and the FBI deal with CT investigations—from the initial intelligence phase into the evidentiary, criminal-justice phase—very similarly. One key difference will undoubtedly remain, however: The UK police will continue to be the agents of executive power. The origins of the Security Service and the FBI were very different, but the work that they need to do today and the way in which that work needs to be done are creating many new parallels in the two organizations. This convergence in their evolution should be viewed as a positive force that may bring about increased international cooperation in countering terrorism.

CHAPTER SEVEN

Domestic Intelligence Agencies After September 11, 2001: How Five Nations Have Grappled with the Evolving Threat

Aidan Kirby

Since 9/11, many nations have struggled with both policy and legal challenges as they come to terms with the rapidly evolving security environment and the role their domestic intelligence agencies should play in it. In their efforts to better prepare for current and emerging threats, some nations have made significant changes to their domestic intelligence structures and practices. The emergence of increasingly sophisticated communication technology; mounting instances of amateur, homegrown terror cells; the prospect of the global diffusion of low-cost yet lethal tactics; and suicide attacks and the use of improvised explosives have combined to make domestic security more complicated. They have also raised questions about the appropriate powers for domestic intelligence agencies in democratic societies. In some countries, efforts to reform intelligence policies in light of these new threats have encouraged governments to redefine key relationships between agencies and adjust the balance between public safety and civil liberties.

In recent years, a number of large-scale attacks have occurred in Western nations and many high-profile plots have been disrupted. These events have affected the ways in which the five nations profiled in this book approach domestic intelligence. The experiences of Australia, Canada, France, Germany, and the United Kingdom provide some insights into the role of domestic intelligence in contemporary CT operations and some of the associated challenges. These cases also

demonstrate that domestic security and intelligence undertakings often have important international implications: When terrorist conspiracies have been carried out successfully, their impacts have often been far-reaching, even contributing to policy actions taken abroad. Examining some of the post-9/11 reactions as they are reflected in intelligence-policy decisions helps provide a sense of how the structures described in this book operate in practice.

Australia

Australia offers an interesting perspective on post-9/11 domestic intelligence and CT, as its allies' experiences have significantly affected its approach. In a reaction to 9/11 and subsequent attacks in Europe, Australia made extensive revisions to its intelligence and security agencies' mandates and powers. Australia itself has been relatively free of terrorist activity within its own borders compared to such nations as the United Kingdom and France. But as Australia has witnessed a series of devastating attacks on other Western nations since 2001, it has responded by continually enhancing the powers of ASIO and redefining the relationship between intelligence and law enforcement. In 2002, Australia began a process of expanding domestic intelligence authorities with the introduction of the ASIO Bill, which was ultimately passed in a revised form in June 2003. The act grants increased powers to ASIO to arrest and detain suspects, including the authority to hold suspects for 48 hours (extendable up to seven days) if the agency has "reasonable grounds for believing that the warrant will substantially assist the collection of intelligence that is important in relation to a terrorism offence" (ASIO Legislation Amendment Act, 2002).

Furthermore, the new legislation dictates that individuals can face a five-year jail term if they refuse to cooperate or answer questions. (Someone can be detained under this new authority even without being an actual suspect—the prospect that a person possesses information about terrorism offenses is sufficient cause.) The attorney general and a federal magistrate or judge can approve a warrant for such detention. The legislation was extremely controversial in Australia, as it drew

ASIO closer to the role of domestic policing and it altered some of the core elements of the existing criminal-justice system.[1]

In November 2003, in the wake of the Bali bombings that claimed 88 Australian lives, ASIO's powers were again revisited and enhanced. ASIO played a key role in the investigation of the attacks, contributing to a 46-member team (which included members of the AFP and state police forces) that traveled to Indonesia to support the local police investigation of the bombings. This attack had a major impact on Australia, paving the way for more revisions to CT law. The 2003 revisions were aimed primarily at protecting intelligence sources and ASIO activities by criminalizing disclosures of information about ASIO warrants, the questioning or detention of a person, or other "operational information" (Anti-Terrorism Bill 2004). Parliament passed a package of espionage laws that strengthened the protections for intelligence sources by providing the same protection to information from international intelligence agencies as is afforded to Australian-sourced information. This was largely an effort to strengthen intelligence cooperation and foster confidence in Australian intelligence and information security among international partners (Grono, 2004).

The Madrid attacks and London bombings in 2005 again prompted action in Australia. Revisions to the Anti-Terrorism Bill 2004 criminalized incitement, outlawed advocating acts of terror (a decision also enshrined in British law in the Prevention of Terrorism Act 2005), and carved out space for preventative detention through lessening the burden of proving a suspect's involvement in a specific plot or target.

Although overseas terrorist attacks have served repeatedly as the impetus for legislative reactions, Australia's confrontation with terrorism has not been confined entirely to vicarious experience. In November 2005, Australian authorities disrupted a major homegrown plot involving 23 men in two separate cells (one in Melbourne and one in Sydney) who were planning wide-ranging attacks. Evidence gathered by authorities suggested that the groups were conspiring to blow up vari-

[1] For a discussion of the post-9/11 legislative changes to ASIO see, Baldino, 2007, and Mahon and Palmer, 2003.

ous targets, including the country's only nuclear reactor, the Australian Stock Exchange, the Australian headquarters of American Express, the Melbourne headquarters of the Department of Foreign Affairs and Trade, and multiple train stations (Madden and Kearney, 2007; Perry, 2005; Stanley, 2005). The raids revealed large quantities of precursor chemicals (the same ones used to bomb the trains in London in 2005), instruction manuals detailing how to construct explosives, and photographs and maps of potential targets (Perry, 2005). It was revealed in 2007 that elements within the network had stolen five shoulder-fired rocket launchers from the Australian Defence Force. The groups had been under close surveillance by ASIO and state and federal law enforcement for 16 months, and the investigation culminated in the largest CT operation in the country's history.

Many of those arrested in Sydney were charged with "conspiring to manufacture explosives in preparation for a terrorist attack," a charge that was created at ASIO's urging only four days prior to the raids through an emergency amendment to the Crimes Act (Stanley, 2005). Despite the significant revisions that had already been made to CT laws, ASIO argued that the current version of the Crimes Act was still too demanding in requiring proof (including details about dates and targets) of involvement in a specific plot. Reports claim that it was the increased frequency of communication between the two cells that acted as the immediate trigger for the November raids (Stanley, 2005). Apparently, the Sydney cell was far more advanced and had reached a higher level of operational sophistication than had the Melbourne cell, and the frequent conversations discussing this fact prompted ASIO to step in when it did.

The post-9/11 expansion of ASIO powers raises important theoretical questions about the role of domestic intelligence in a democratic society. Some have expressed concern that ASIO's new powers are inappropriate for an intelligence agency, arguing that the authorities reach too far in permitting the agency to direct the detention of individuals who are not suspected criminals or terrorists but may simply have come into contact with valuable information. The expanded ASIO provisions render detention and interrogation tools of intelligence *gathering*, an application far different from the powers' original purpose. Austra-

lia's domestic intelligence capability can still be described as lacking law enforcement powers, but the series of expansions made to ASIO's powers since 9/11 has certainly changed the nature of the service's role and made the division less distinct in practice. Australia's series of legal revisions also demonstrates the power of global events in helping to construct a new perspective on domestic threats.

Canada

Like Australia, Canada's current approach to domestic intelligence has been shaped in part by its closest allies' direct experiences with terrorism. In the immediate aftermath of 9/11, Canada reacted by making significant changes to the legislative foundation of its intelligence and CT work. Prior to the December 2001 introduction of the Anti-Terrorism Act of Canada (Bill C-36), there was no legal basis for officially listing entities as terrorist groups or criminalizing association with such groups. The act also conferred new powers to security and law enforcement, including the authority to hold investigative hearings, compel testimony, and conduct surveillance, and provided for preventive detention and restrictions on disclosure rules under the Canada Evidence Act. Unlike Australia, whose legislative reforms emerged gradually over an extended period, Canada's response was the creation of an omnibus act that included an extensive package of new powers aimed at better preparing Canada for the post-9/11 security landscape. Some feel that the act's size and scope, combined with political urgency, led to the rushed passage of a bill that received relatively little scrutiny (Gabor, 2004).

Canada has been largely spared the struggles with domestic terrorism that some of its European allies have faced. Thus, it was a number of years after the passage of C-36 before the act's utility and implications were publicly demonstrated. In the summer of 2006, however, CSIS, in cooperation with the RCMP, disrupted its first incidence of post-9/11 era homegrown terrorism. The investigation revealed an elaborate plot involving 17 men who planned to storm Parliament, kidnap politicians, behead the prime minister if he refused to pull Canadian troops

out of Afghanistan, detonate truck bombs in downtown Toronto, and, ultimately, open fire on any survivors. The extent of the plans and the identities of those involved became clear largely through email and phone conversation monitoring, but CSIS also leveraged HUMINT sources by placing a mole from the local Muslim community inside the cell (Friscolanti, Gatehouse, and Gillis, 2006). Reports suggest that Canada was initially made aware of the possibility of the development of a Canadian cell in 2005, when British authorities shared intelligence about the online activity of Younes Tsouli (aka Irhabi 007), a London man involved in the operation of many radical Web sites.[2] Tsouli was apparently communicating with individuals in Toronto and Atlanta in one of his chat rooms. Shortly thereafter, CSIS alerted the RCMP of its concerns, at which point a criminal investigation was opened and sustained surveillance began.

Measures introduced with the Anti-Terrorism Act of 2001 proved important in handling this case. Investigators could monitor a broader network of individuals because of the law's recognition of the importance of facilitators in terror plots. The act also removed some obstacles to electronic surveillance operations, and this was perhaps the most significant provision, as electronic surveillance has become such an integral component in the early detection of terrorist activity. Prior to 2001, investigators would have been denied the access that, in this investigation, allowed government teams to intercept phone, computer, and wireless communications for as long as a year without renewing their warrants. The act also absolved the intelligence and security communities of the responsibility to convince a judge that wiretapping was, in fact, a last resort.

The passage of the Anti-Terrorism Act was an important legislative development in shaping the domestic security and intelligence capabilities in Canada. But even in light of these enhanced authorities, CSIS faces challenges in meeting its intelligence requirements because it operates in the absence of a complementary foreign intelligence–collection capability. The question of how to confront the increasingly global nature of contemporary security threats with the limited man-

[2] For an account of Tsouli's activities, see Katz and Kern, 2006.

date of collecting only domestic intelligence is clearly a complicated one. Although the 2006 plot was primarily a domestic incident, the initial intelligence provided by the UK was instrumental. This underscores the difficulty in trying to draw strict distinctions between "domestic" and "foreign" intelligence.

The CSIS Act of 1984, which lays out CSIS's authorities, is ambiguous in some respects, and this has caused confusion and legal debate in the evolving security climate. It gives the agency the authority to investigate threats "within or relating to Canada" but elsewhere explicitly restricts the gathering of information about foreign states.[3] This issue was recently raised in a case when the Federal Court of Canada rejected warrants that would have allowed CSIS to intercept telecommunications involving a number of suspects who were Canadian citizens residing in foreign countries (McGregor, 2008).

Scholars have argued that this type of ambiguity should not be permitted to continue and that CSIS's powers to operate abroad in investigating threats to Canada must be clarified. A clearer mandate for CSIS may affect the more serious question of creating a separate foreign intelligence agency. There continues to be ongoing political discussion in Canada of ways to strengthen CSIS's role both domestically and abroad while strengthening parliamentary oversight mechanisms (Maccharles, 2007). As the line between domestic and foreign threats becomes increasingly obscured through the rapid movement of people and information and by the transnational character of today's terrorist threat, the traditional mandate of CSIS may prove difficult to sustain.

France

France's unique approach to domestic intelligence and security has been heralded for its effectiveness in CT operations (Gerecht and Schmitt, 2008; Block, 2005). It has also been argued that while the UK and

[3] While CSIS does not have a mandate to collect foreign intelligence per se, it does station some officers overseas who fulfill a partial external collection function and act as liaison officers with foreign agencies.

Germany were relatively slow to awaken to the threat of homegrown Islamic extremism, France's experiences in the 1980s and 1990s helped to enshrine effective measures for dealing with this type of domestic threat (Block, 2005). But as arguably the strictest domestic intelligence regime in Europe—and one that often relies on such measures as preemptive arrests and ethnic profiling—the system has also received much criticism for its apparent willingness to marginalize civil rights in the fight against terrorism (Sciolino, 2008; Whitlock, 2004).

One of the attributes of the French intelligence structure that distinguishes it from its Western counterparts is the privileged relationship between intelligence services, especially the DST, and the magistrates known as *juges d'instruction*. Both parties are granted highly intrusive powers of surveillance and the magistrates oversee and even direct the investigative activities of the intelligence unit of the French national police and the DST. Because of the unique relationship between the intelligence community and the magistrates, the state's CT prevention and repression powers are highly coordinated and concentrated even though intelligence and law enforcement are separated in theory.

Because of its history of dealing with domestic terrorism threats, France did not, unlike Australia and Canada, dramatically reform its intelligence and legal practices after 9/11. France's formal approach has been relatively consistent in the past decade, but relationships and cultures, such as the style of cooperation between the DST and the magistrates, have evolved. One major organizational change that occurred within France's domestic security apparatus was collocating the DST, the DCRG, and the DNAT in 2006 in hopes of better coordinating and streamlining operations. French leadership continue to be introspective when it comes to CT and intelligence policy, continually seeking to better align the nation's resources to the adapting threat. A 2006 government white paper on domestic security against terrorism was released to articulate and codify a comprehensive security strategy motivated largely by the attacks in Madrid and London in the preceding two years (Premier Ministre, 2006). The first chapter, entitled "Surveillance, Detection, and Neutralization," explicitly addresses the fact that the French penal system does not recognize a rigid separation

of prevention and punishment and characterizes this attribute as an important strength in facing the mutating threat of terrorism.

France has faced an increasing pace of domestic terrorist activity in recent years. One of the largest disruptions of an ongoing plot occurred in 2005 in an operation directed by the antiterrorist magistrate Jean-Louis Bruguière. The operation involved significant interagency cooperation and was conducted jointly by the DST, detectives from France's organized-crime unit, and members of the country's police paramilitary force (Sciolino, 2005). The 20 people arrested in December 2005 included both Islamic militants and petty criminals and the conspiracy appeared to combine petty crime (as a fundraising mechanism) with plotting a large-scale act of terrorism.

Much like the United Kingdom and Germany, France faces domestic intelligence challenges shaped in part by the demographic makeup of its population. France has the largest Muslim minority in Europe, so effectively monitoring the public for security threats without alienating and potentially radicalizing segments of French society requires a delicate balance. One specific program long used by the French in the effort to root out radicalism at early stages is the mosque surveillance program (Combelles Siegel, 2007). In hopes of stemming the circulation of violent and radical ideologies inside France, the DCRG has been monitoring mosques, their clerics, and sermons since the 1990s. Through close surveillance of its approximately 1,700 mosques, the French hope to preempt the development of terrorist activity by determining which imams advocate radical viewpoints and exploring whether any of these mosques serves as a center of terrorist support or operational planning. France has had a law authorizing the administrative expulsion of radical foreign imams for many years. With this judicial foundation, the DCRG can inform police of evidence gathered in surveillance, at which point the police can summon the cleric and threaten him with expulsion. The close relationship between intelligence and law enforcement helps programs like this one function effectively in France.

France's secular political culture and organizational structures make highly intrusive surveillance programs like this one reasonably effective. But in other societies, such approaches to dealing with similar

challenges (such as indigenous radicalism) are considered less appropriate and are less likely to be accepted by the general population. For instance, in the aftermath of the London bombings of 2005, when Finsbury Park Mosque emerged as a key point of interest because it linked together the bombers and other known radical elements, then–French Interior Minister Nicolas Sarkozy publicly suggested that the French mosque-surveillance program might benefit Britain as well. However, British Home Secretary Charles Clarke immediately rejected the idea, claiming that the program was probably more appropriate for France and underscoring how important it was to "work with the legitimate mainstream Muslim community and . . . not alienate what they do" ("UK Rejects Sarkozy's Mosque Surveillance Plan," 2005).

Germany

Germany faced difficult questions about its domestic intelligence structure in the aftermath of 9/11. Having housed the members of the Hamburg cell within its borders for years, and having failed to uncover the nature of the cell's plans and activities in time to prevent 9/11, Germany was forced to examine some of the issues that received so much attention in the United States: Why had the dots never been connected? To what extent could such intelligence failures be avoided in the future through organizational changes?[4] Like the other countries discussed in this book, Germany made some immediate legislative changes to address the major loopholes that permitted terrorists to operate freely inside the country (Miko and Froehlich, 2004). Religious groups and charities ceased to enjoy immunity from investigation or surveillance by the government and terrorists became eligible for prosecution in Germany even if they belonged to foreign terrorist organizations that did not target Germany.

The organizational structure of Germany's intelligence community presented challenges to its post-9/11 reform efforts. However, Germany's intelligence structure was highly decentralized at the end of

[4] For an account of the Hamburg cell's activities leading up to 9/11, see Finn, 2002.

World War II, and when the Allies defeated the Nazis, they broke up many of the national security agencies to prevent a resurgence of the Gestapo. Police were banned from gathering domestic intelligence, so each *Land* created its own intelligence agency. These state agencies coordinate with each other to an extent, but each reports directly to its own state government. This structure is extremely complex and can inhibit timely information sharing and complicate both domestic and international cooperation in the current security environment.

Even the federal-level agency headquarters are distributed throughout the country. The BND, Germany's federal intelligence service, is in Berlin; the BKA, the federal criminal police, is headquartered in Wiesbaden;[5] the BfV, Germany's domestic intelligence agency, is based in Cologne. While modern technology certainly helps to facilitate remote communication, the geographical dispersion of agencies that need to work so closely in the event of a crisis has been raised as a potential problem should a major incident arise in Germany.[6]

The events of 9/11 first prompted German policymakers to seriously reconsider the country's domestic intelligence structure and the Madrid attacks in 2004 only underscored this need. In the aftermath of Madrid, some conservative politicians advocated abolishing the 16 different BfV bureaus in favor of creating a unified federal authority ("Germany to Revamp Domestic Intelligence Service," 2004). But as with any bureaucratic organizational undertaking, the various stakeholders viewed this proposal differently. Some small states were more willing to give up their autonomy, immediately recognizing the potential benefits (in terms of gaining much-needed resources and skills), but, unsurprisingly, larger states were disinclined to give up powers and instead favored maintaining the status quo (Miko and Froehlich, 2004).

A major plot disrupted in 2007 through U.S.-German intelligence cooperation presented an opportunity to review existing German structures in the context of real events. In September 2007, two German

---

[5] Note, however, that the BKA's CT unit is in Meckenheim, near Bonn.

[6] See Boston, 2004, for a discussion of Germany's domestic intelligence structure and post-9/11 challenges.

converts to Islam and a Turkish national were arrested in the act of mixing chemical ingredients to make explosives apparently intended to be used in car bomb attacks on a U.S. military base in Germany, a nightclub, a German airport, or other targets (Kaiser, Rosenbach, and Stark, 2007). The arrests concluded a nearly yearlong investigation involving close cooperation among the U.S. National Security Agency (NSA) and various German intelligence authorities. The investigation, code-named Operation Alberich, was conducted from both Berlin and Washington, with cooperation being facilitated through a joint CIA and German task force in Berlin (Kaiser, Rosenbach, and Stark, 2007). U.S. officials were highly invested in monitoring the group, partly due to fears that the ultimate target might be the United States. The investigation involved high levels of surveillance by the BKA and close work between the BKA and the BfV, although the two organizations disagreed at times about the nature of and motivations behind the plot. The domestic intelligence gathered in Germany was supplemented by the intelligence contributed by the CIA and the NSA, which consisted of intercepted messages between German Islamists and militant contacts in Pakistan. Ultimately, the disruption of the plot helped encourage greater political consensus in Germany about the value of increased surveillance powers (Kaiser, Rosenbach, and Stark, 2007). The investigation's success did not provide any definitive answer to the question of whether Germany would benefit from a more highly centralized domestic intelligence structure. However, the important role of the U.S.-German task force in Berlin does suggest that a single point of coordination for the investigation and disruption of large-scale terrorism planning (especially when the investigation involves international cooperation) is a highly valuable, if not crucial, element.

United Kingdom

Of all the Western domestic intelligence agencies, the UK's MI5 is perhaps the best known. It has also been submitted to the greatest amount of public scrutiny in recent years, largely due to its failure to prevent the train bombings in July 2005 that killed 52 people. Although MI5

is an extremely mature and well-resourced organization that has dealt with the phenomenon of domestic terrorism for decades, it has faced significant challenges in adapting its practices and mind-set to a new type of overarching threat.

The suicide attacks of July 2005 shocked the politically tolerant and multicultural nation. Although the domestic intelligence and law enforcement communities were well aware of the presence of radical Islamic elements in the UK prior to the bombings, the scale of the attacks and the revelation that all four of the attackers were British signaled that the threat had reached a new threshold and a new level of complexity. When it became public that two of the 7/7 bombers had actually come across MI5's radar prior to the attacks on the "periphery of other investigations," the question of why this discovery had not led to the plot's disruption naturally followed (Intelligence and Security Committee, 2006).

According to the report published by the UK ISC in May 2006, the circumstances under which the two plotters, Siddeque Khan and Shazad Tanweer, had emerged during earlier investigations did not merit further investigation in light of the many other competing priorities that the service faced. The intelligence available at that time had revealed that meetings were taking place but did not give any indication that these meetings were related to the planning of a terrorist attack (Kaiser, Rosenbach, and Stark, 2007). One of the findings of the parliamentary panel's report on the attacks was reminiscent of the 9/11 Commission's conclusion that the intelligence failures leading up to 9/11 stemmed in large part from a "failure of imagination" (9/11 Commission, 2004). In its review of the 7/7 attack, the parliamentary panel found that the failure of the UK intelligence community to detect and disrupt the attack had not been the product of any one isolated error or oversight. The problem was higher-level and more widespread: "We remain concerned that across the whole of the counter-terrorism community the development of the home-grown threat and the radicalization of British citizens were not fully understood or applied to strategic thinking" (Intelligence and Security Committee, 2006).

Since the 7/7 attacks, the United Kingdom has continued to be a target for radical Islamists and MI5 has faced a steady stream of both

domestic and international conspiracies. In November 2006, Eliza Manningham-Buller, the MI5 DG, stated that there were an estimated 1,600 suspected terrorists involved in at least 200 networks in Britain. In February 2007, MI5 admitted that there had been twice as many plots disrupted in the UK since the 7/7 bombings than had actually been made public—on average, one plot every six weeks (Jordan, 2006; Rayment, 2007).

One of the largest and most publicized of the interrupted terrorist conspiracies in the post-9/11 era took place in the summer of 2006 in what has become known internationally as the "liquid bomb plot." This case involved 29 men, mostly second- or third-generation British citizens of Pakistani descent, whose goal was to break into smaller cells and then smuggle peroxide-based liquid explosives and detonators onto nine planes flown by four carriers flying direct routes between the UK and the United States. The liquid bombs would have been detonated midair and, according to intelligence officials, would have killed as many as 2,700 people (Bennett and Waller, 2006). The plot was ultimately disrupted at a point near execution but the attack was not imminent. This reflects British CT policy's increasing emphasis on prevention since 7/7, even at the expense of gathering additional evidence that could be of use in legal proceedings (see Gregory, 2005; Klausen, 2007).

MI5 and Scotland Yard had been tracking the development of these plans for many months leading up to the arrests and the intelligence gathered on the ground by British intelligence was further clarified by U.S. contributions of communication intercepts. The highly sophisticated surveillance operation involved covert raids on the homes of key terrorism suspects and planting bugs to gather definitive intelligence on the details and planned timing of the plot (Lewis, 2006). The investigation also involved close U.S.-British cooperation, but when it came time for British authorities to intervene, U.S. authorities would not allow U.S. airports to be notified until all the arrests were complete.

Despite the highly intrusive nature of this operation, MI5 continued to operate within its standard oversight mechanism: Approval was gained from the home secretary, and, over the months of the investiga-

tion, then–Home Secretaries Charles Clarke and, later, John Reid were each given regular detailed updates on the investigation's progress. Although the United Kingdom has faced perhaps the greatest challenge among the countries discussed here in terms of sheer numbers of plots, it appears the least eager to radically change its legal foundations. Instead, British responses have focused more on increasing intelligence-community resources and on the institutionalization of longer-term strategies of prevention, specifically those aimed at addressing underlying causes of alienation ("Preventing Terrorism Together," 2005).

Conclusion

In comparing these five nations' experiences, it becomes clear that the post-9/11 era has raised many new and challenging questions about the role of domestic intelligence agencies. Although each of the countries discussed has, at times, faced similar threats, each has approached the challenges from a perspective shaped by a distinct historical context and a specific political culture. These factors have influenced the choices available to policymakers and have thus shaped the systems and structures that have emerged. Each system is unique, but several common themes can be discerned when examining these post-9/11 experiences comparatively.

At the most basic level, these cases demonstrate that simply having a domestic intelligence service is no panacea for eliminating domestic threats. In this group of countries, there are examples of both disrupted and successfully executed attacks. Each country's intelligence agencies have played important roles in monitoring domestic threats, especially as homegrown radicalism has developed as a significant national security concern in recent years. However, many factors affect a nation's ability to improve overall security and the mere existence of a domestic intelligence agency clearly provides no guarantee against domestic terrorism.

The struggle to define the proper relationship between law enforcement and intelligence has emerged as a common factor. As threats to national security evolve and become more sophisticated, the once

clear-cut distinction between the two communities has been deliberately relaxed in many national contexts. The significant adjustments that have been made to the relationship between law enforcement and intelligence raise questions about the natures of both missions and how separate these disciplines can actually be in CT operations. There are many good reasons for dividing these public safety functions institutionally, but the reforms discussed in this book and the tensions that have emerged during these periods of change reveal the inherent connections between the two missions. Many examples exist of effective intelligence agencies that are given some degree of law enforcement powers and of law enforcement agencies that play a role in intelligence gathering. It is not surprising that, in the current context, many countries have sought to make this division less rigid. But such decisions clearly have complex political implications that are still becoming fully understood.

On a more operational level, many of the new powers explored in this book relate primarily to the expansion of surveillance authorities, which, in practice, translates into enhanced collection capabilities. Many of the intelligence successes discussed in preceding chapters do appear to have depended at least in part on the discoveries made through this enhanced collection. However, it is important to recognize the analytical challenges that are introduced when agencies are empowered to gather more intelligence. For instance, MI5's failure to recognize the pre-attack activity of two of the 7/7 plotters as suspicious at an early stage demonstrates that robust surveillance powers must be married to a highly efficient analytical capability and an accurate picture of the security environment at the strategic level.

The issues of oversight and accountability become ever more important as agencies are awarded increasingly intrusive powers. Each of the countries examined in this book approaches the issue of oversight differently. For example, Canada has perhaps the most comprehensive mechanism of institutionalized oversight, followed by the UK and Australia; France's system is considerably less rigorous. In the post-9/11 context, there is evidence of an impulse to reduce the interference of oversight mechanisms in antiterrorism legislation, as was seen in Australia. However, other nations, such as the UK, have avoided

such an approach, aiming instead to strengthen their agencies' operational abilities within the preexisting accountability structures. Recent debate in Canada suggests that the aims of broadened powers and enhanced accountability are actually being pursued simultaneously in that country.

Lastly, these cases all demonstrate the international dimension of domestic intelligence. Although the countries' agencies operate mainly within the confines of their own borders, they also operate within the context of international security developments. Domestic incidents that have taken place in one nation have often caused changes in threat perceptions abroad in significant ways; these changes have, in turn, influenced major policy changes. Furthermore, the distinction between intelligence that is strictly domestic and intelligence that is also (or solely) international has become harder to make. In this era of transnational threats, domestic intelligence activities are often fused with international intelligence products, and major successes may rely on significant elements of international cooperation. In this sense, these five nations' post-9/11 experiences are connected in important ways and their unique struggles and approaches can be best understood in a comparative context.

CHAPTER EIGHT

Conclusions: Lessons for the United States

Peter Chalk, Lindsay Clutterbuck, Brian A. Jackson, and Richard Warnes[1]

In considering the creation of a domestic intelligence agency in the United States, the experiences of other countries that already have such agencies can be instructive. However, differences in the legal, social, and historical circumstances in those countries and in the public's attitude and reaction to intelligence and security efforts—among other idiosyncrasies—make it impossible to simply extrapolate the experiences of others and use them to predict the best way of creating such an organization in the United States. This approach would also not be able to accurately gauge whether the organization would be successful if it were created or whether even a successful organization would be acceptable to the public. Looking across the five case studies of democracies with stand-alone intelligence agencies does, however, suggest some common themes:

- Most of the countries have seen explicit value in placing domestic intelligence-gathering activities in agencies that have no law enforcement powers of arrest or detention. This separation facilitates intelligence-gathering efforts but poses challenges when prosecuting individuals for terrorism-related offenses is necessary.
- Most of the nations with domestic intelligence agencies have a system of external oversight, often by multiple bodies, that, in principle, acts as a check on the agencies' potential power.

[1] This discussion was crafted from the contributions made by each listed author. Author names are presented in alphabetical order.

- Although many concerns about domestic intelligence focus on the effect that such activities can have on individuals and communities, in several countries, community liaison is an important and integral part of the agencies' efforts to achieve their missions.
- Although the national-level domestic intelligence organization may play a very central role in CT activities, the breadth of the CT mission requires extensive interaction with other intelligence and law enforcement organizations and, in some cases, formal regional or federated structures of component organizations to "cover" the entire country.
- In spite of a desire in the past to maintain a clear organizational division between domestic and foreign intelligence activities, some countries' domestic intelligence agencies explicitly sought—sometimes even initiating their own collection efforts—to gather information internationally given the transnational nature of the contemporary terrorism threat. In an increasingly interconnected and globalized world, the boundary between what is "domestic" and what is "foreign" has become increasingly blurred and hard to define coherently. This dilemma is reflected in the efforts of countries to apportion who does what in the field of CT intelligence.

The following sections briefly explore each of these themes, drawing on examples from the case studies.

Separation of Domestic Intelligence from Law Enforcement Authority

Across the case studies, the separation of law enforcement or arrest and detention authority from domestic intelligence is a common feature. This separation results in a range of advantages. First, it ensures that the decision to arrest and prosecute an individual does not lie solely in the hands of the organization that has gathered intelligence about that person's activities. Instead, the police decide—after consultation with intelligence services and state prosecution authorities—whether to make an arrest. The national criminal-justice system undertakes any

subsequent prosecution, which thus comes under the scrutiny of the judiciary. The police work in conjunction with the intelligence services to build an evidential case, using intelligence that the intelligence service has gathered as evidence when it is appropriate to do so but also seeking their own evidence. Consequently, checks and balances exist to ensure that the nation's intelligence services cannot detain and hold any individual without the involvement of the national criminal-justice system. In this way, individual human rights are protected and the country's duty to protect its citizens is upheld, In fact, this separation may even strengthen the intelligence agency's democratic acceptability to the public.[2]

At the operational level, the existence of bureaus that can devote their full resources to preemptive information gathering, analysis, and dissemination is a positive feature. In Australia, Canada, and the UK, separating law enforcement from domestic intelligence—and placing these functions into dedicated agencies specifically mandated to carry out each task—has certainly helped alleviate the problem of competing functional demands. Just as importantly, it has allowed preemptive investigations to proceed without a criminal offense having been committed and without the pressure to quickly move resources elsewhere when hard evidence is not forthcoming. This has facilitated extended surveillance of some terrorism suspects and kept the agencies focused on the long term threat posed by individuals or groups. Ultimately, the separation of security intelligence and policing in these three countries reflects what might be called a *culture of prevention* with respect to terrorism (see, e.g., GAO, 2000, p. 8). Indeed, ASIO, CSIS, and MI5 have all developed an over-the-horizon perspective on the respective terrorist threats they face and been able to devote substantial resources to honing analytical capabilities, in-house foreign-language skills, and subject-matter expertise on particular groups and their motivations. Some suggest that the separation has also contributed to the agencies' ability to draw on a wider, more diverse intelligence-analyst recruit-

[2] For example, this consideration was central in the decision to set up CSIS.

ment pool,[3] thereby allowing the agencies to improve their analytical capabilities and quality.

However, while separation has strengths, each agency does have to navigate a hand-off between intelligence and law enforcement when the time comes to prosecute individuals for terrorist offenses. They also face challenges regarding the use of intelligence information for investigation and evidentiary purposes. For intelligence to lead to prosecution, this hand-off must occur even if domestic intelligence functions are collocated with law enforcement powers within the same organization; when the two are separated, however, the hand-off crosses organizational boundaries rather than the divisions between units in the same organization. Close cooperation and interaction between the intelligence agency and law enforcement organizations have resulted from this challenge in some of these countries and produce benefits of their own, but does not in all cases eliminate the inherent tensions that exist between the police, whose overriding mission is public safety, and the intelligence agencies, whose overriding mission is national security. In the UK, the presence of special branch officers to help bridge this gap was cited as critical; in France, the majority of domestic intelligence officers are seconded directly from the national police.

The Canadian example also suggests that divesting the police of a preexisting intelligence function and placing that function in the hands of a new, separate body could cause a degree of interagency friction, if not outright hostility. The years immediately following the creation of CSIS were marked by a period of tangible antipathy between the service and the RCMP, and this antipathy directly impeded effective bilateral collaboration and information sharing. Indeed, the board of inquiry that investigated the Air India bombing of 1985—Canada's worst mass murder—concluded that the attack reflected a massive "failure of the system" and the wholesale failure of the security and police services to work together to preempt an avoidable disaster ("Police Had Hint 11 Days Before 1985 Air India Bombing," 2007; "Canadian Agencies

[3] Including individuals—such as linguists, historians, social scientists, psychologists, economists, and country or regional experts—who might not normally be interested in entering a law enforcement profession.

Were Warned of Air India Attack in Advance," 2007). Canada's experience speaks directly to the potential organizational birth pangs that could arise in the United States should a decision be made to set up a new domestic intelligence agency. Given the complex array of immediate threat exigencies confronting the country in the post-9/11 era, these are something that Washington can ill afford.

External Oversight

In many of the case studies, institutions and structures for external oversight that provide a check on an intelligence agency's potential power are a key element of the overall domestic intelligence system. For example, in Australia and Canada, although the primary oversight, review, and audit power rests with the executive, there are also royal commissions and official boards of inquiry. And, crucially, at the parliamentary level, these oversight bodies have been integral to appraising ASIO and CSIS policy, finance, and administration and ensuring that the agencies' operational programs and resources are implemented and used in as effective, efficient, and legitimate a manner as possible. German domestic intelligence and internal security systems are also subject to rigid parliamentary and administrative control and oversight. The UK has a variety of oversight structures, although legislative oversight is somewhat less stringent because ISC is both appointed by and answers directly to the prime minister. France differs somewhat from the other cases in this respect: There is less effective parliamentary oversight, due in part to the historic legacy of the Communist Party's previous involvement in government.

In considering the *effectiveness* of oversight in the various nations, conclusions must be drawn cautiously. Most cases provide examples of oversight actions taken when problems became public, although no case study based on open-source data and conducted from the outside can provide any certainty about whether those examples are representative (of either the actions of usually secret intelligence organizations or their overseers) or aberrant.

Community Interaction and Liaison

In the ASIO and CSIS cases in particular, a key part of domestic intelligence agencies' information gathering has relied on overt community liaison. These activities have availed a useful force-multiplier effect that has not only greatly enhanced the potential scope of national surveillance efforts but also afforded a direct conduit for assessing the residual threat emanating from co-opted, homegrown extremism. Moreover, because meetings and interviews have frequently been held open to the public, they have helped give the two intelligence services more of a public face and an opportunity to explain the nature, rationale, and purpose of their work. The value-added dimension of this latter aspect should not be ignored. Many Australian and Canadian immigrants come from countries where internal security agencies have earned reputations for arbitrariness, brutality, and corruption. Their natural inclination, therefore, is to view the intelligence community writ large as a community bereft of civil responsibility and professionalism. Systematically moving to break down these negative perceptions and suspicions has been vital to winning the trust of these communities and gaining their support for CT efforts.

Community liaison is obviously a highly important consideration in the United States, especially given the large number of immigrants in the country (many of whom come from areas of the world beset by serious problems of extremist violence). Working at the grassroots level to better understand the fears, biases, and social dynamics that drive or otherwise influence the actions and thinking of ordinary individuals is now generally viewed as indispensable to any viable CT campaign and is explicitly recognized in Washington's 2007 National Strategy for Homeland Security (see Homeland Security Council and Bush, 2007, pp. 22–23). Of course, this is not to say that community liaison would be any better served by a separate intelligence service. However, if such an agency is developed in the United States, it is critical that its functional mandate extends to and embraces concerted grassroots dialogue and engagement.

Cross-Agency International and Regional Structures

In virtually all of the case studies, the inability of the central domestic intelligence agency to "cover everything" has led to interaction with other agencies. Some of this interaction is due to the previously discussed tensions between police and law enforcement authority, but in many cases, cooperation with partners is a key source of information and other capabilities. Partners include other members of the national intelligence community and, in some cases, organizations from other countries.

The need to fully cover just their own countries has led some agencies to adopt regionalization or federated structures for information gathering and other activities. Some of these activities have occurred through liaison with national, regional, or local police agencies (e.g., the special branches in UK police organizations), but in others, the domestic intelligence agencies have their own regional structure.[4] This is particularly the case in Germany, where the BfV organization is linked to the regional LfV offices in each of the 16 *Länder*, each of which is independently responsible for domestic intelligence and internal security within its state. The structure of the BfV organization—regional LfV offices in each *Land* are independently responsible for domestic intelligence and internal security within that state yet linked to and reporting information back to the federal BfV in Cologne—could be a useful template for any planned domestic U.S. intelligence service. Although such a network in the United States would clearly have to be far more expansive, the principle of the German structure appears sound. In a U.S. model, the LfV concept might be replicated by creating a regional domestic intelligence office in each of the 50 state capitals. These offices would be linked electronically by a system similar to NADIS and would report to a centralized headquarters, possibly based in Washington, that replicates the BfV. However, one clearly

[4] It is interesting to note that the UK Security Service has, since 2001, reorganized itself away from having a permanent presence only in London to establishing a series of regional offices throughout the UK. For the first time in its history, the service now has a national presence that matches its national responsibilities. This change has also increased and improved the service's liaison with regional and local special branches.

problematic aspect of the German model is the BfV's lack of direct and overarching control of the various LfVs. Thus, in a U.S. version, any independent state-based domestic intelligence offices might need to be placed under more-direct legal and practical control and coordination from a federal headquarters organization. Such a model is not dissimilar to the existing FBI field office and Field Intelligence Group structure (complemented by joint terrorism task forces and fusion centers).

An additional potential benefit of applying such a system to the United States would be that it helps solve a difficulty that results from the country's large size: It remains difficult for any one organization to perform effective domestic intelligence oversight. The delegation of responsibility from a federal-level headquarters to state-level offices responsible for domestic intelligence and internal security within their own states would help ensure that local awareness and knowledge could be brought to bear. Equally, local concerns, which can develop into national threats, would be much less likely to slip through the cracks. At the same time, such a devolved structure would help facilitate closer cooperation between the state offices and state- and local-level police and law enforcement bodies.

A Blurred Boundary Between Domestic and Foreign

The creation of a new domestic intelligence agency in the United States would presumably be intended to consolidate and build on the country's existing domestic intelligence–gathering effort and thus help solidify the line between domestic and foreign intelligence. However, the case studies suggest that in sharpening this division, caution is warranted. Although ASIO and CSIS in particular act primarily as domestic intelligence services, each has had to adopt a broader international focus given the transnational nature of contemporary terrorism. As noted in Chapter Three, CSIS's situation is unique and special in this regard, largely because Canada does not have an external intelligence-collection service comparable to the foreign intelligence-collection agencies in the other four countries. If a new intelligence agency were created with the primary responsibility for CT, it would face the lion's share of

criticism when successful attacks occurred in spite of its efforts. Thus, it would not be surprising for that agency to desire access to foreign intelligence and intelligence about domestic, nonterrorist activities. If a new agency in the United States developed those, effective cooperation and coordination between it and other agencies in the foreign intelligence community would at a minimum be required, as would collaboration between services involved in general intelligence-gathering activities and those with a dedicated CT role.

References

9/11 Commission—*see* National Commission on Terrorist Attacks upon the United States.

AAT—*see* Administrative Appeals Tribunal.

Action Directe, "Communiqué on the Assassination of General René Audran, Director of International Affairs at the French Ministry of Defense in Paris on 25 January 1985," in Yonah Alexander and Dennis A. Pluchinsky, eds., *Europe's Red Terrorists: The Fighting Communist Organizations*, London and Portland, Oreg.: F. Cass, 1992, pp. 140–141.

Administrative Appeals Tribunal, home page, undated. As of June 12, 2007: http://www.aat.gov.au

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Implementing the National Strategy: Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction*, Washington, D.C., 2002. As of October 10, 2008: http://purl.access.gpo.gov/GPO/LPS25391

AFP—*see* Australian Federal Police.

AG—*see* Attorney-General's Department.

"Analysis: German Suspects in Afghanistan," United Press International, May 1, 2008.

ANAO—*see* Australian National Audit Office.

Anderson, James H., "The Neo-Nazi Menace in Germany," *Studies in Conflict and Terrorism*, Vol. 18, No. 1, 1995, pp. 39–46.

Andrew, Christopher M., and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*, New York: Basic Books, 2001.

Anti-Terrorism Bill 2004—*see* Parliament of the Commonwealth of Australia, House of Representatives (2004).

ASIO—*see* Australian Security Intelligence Organisation.

ASIO Legislation Amendment Act 2002—*see* Parliament of the Commonwealth of Australia, House of Representatives, 2003.

"ASIO Mole Sold Secrets to KGB," ABC News Online, November 2, 2004. As of October 23, 2008:
http://www.abc.net.au/news/newsitems/200411/s1232385.htm

Attorney-General's Department, "Mercury '05: Questions and Answers," Web page, undated. As of April 30, 2007:
http://www.ag.gov.au

Attorney-General's Department, "New Counter-Terrorism Intelligence Centre Launched," press release, October 17, 2003.

Aussaresses, Paul, and Robert L. Miller, *The Battle of the Casbah: Terrorism and Counter-Terrorism in Algeria 1955–1957*, 3rd English ed., New York: Enigma, 2006.

Austen, Ian, "In Break from History and Scandal, Canada Chooses a Civilian to Lead the Mounties," *New York Times*, July 7, 2007a. As of October 23, 2008:
http://www.nytimes.com/2007/07/07/world/americas/07canada.html

———, "Deported Canadian Was No Threat, Report Shows," *New York Times*, August 10, 2007b. As of October 23, 2008:
http://www.nytimes.com/2007/08/10/world/americas/10arar.html

"Australia to Double Spy Personnel," BBC News, October 16, 2005. As of October 22, 2008:
http://news.bbc.co.uk/2/hi/asia-pacific/4347352.stm

"Australia Nabs 16 in Terror Raids: Police Say They Foiled Attack in String of Major Raids," CBS News, November 7, 2005. As of February 8, 2006:
http://www.cbsnews.com/stories/2005/11/07/terror/main1021256.shtml

Australian Federal Police, *Annual Report 2005–06*, Canberra, 2006. As of October 22, 2008:
http://www.afp.gov.au/__data/assets/pdf_file/24502/AR_05_06.pdf

Australian National Audit Office, home page, undated. As of June 12, 2007:
http://www.anao.gov.au

Australian Security Intelligence Organisation, *Report to Parliament 2004–2005*, Canberra: Australian Government Publishing Service, September 2005. As of October 22, 2008:
http://www.asio.gov.au/Publications/Content/AnnualReport04_05/pdf/asio_annual_report_to_parliament_0405.pdf

———, *Report to Parliament 2005–2006*, Canberra: Australian Government Publishing Service, September 2006. As of October 22, 2008:

http://www.asio.gov.au/Publications/Content/AnnualReport05_06/pdf/ASIO%20annual%20Report%20to%20Parliament%2005-06.pdf

———, *Corporate Plan 2007–2011*, Canberra: Australian Government Publishing Service, 2007a. As of October 22, 2008: http://www.asio.gov.au/Publications/Content/Corporateplan/Contents/CorporatePlan.aspx

———, *Report to Parliament 2006–2007*, Canberra: Australian Government Publishing Service, September 2007b. As of October 22, 2008: http://www.asio.gov.au/Publications/Content/AnnualReport06-07/pdf/ASIOAnnualReport0607.pdf

Baldino, Daniel, *Good Instincts or Poor Judgment? Australia's Counter-Terrorism Response After 9-11*, presented at 2007 Australasian Political Studies Association conference, Monash University, Melbourne, Australia, September 24–26, 2007. As of October 28, 2008: http://arts.monash.edu.au/psi/news-and-events/apsa/refereed-papers/au-nz-politics/baldino.pdf

Baud, Jacques, *Encyclopédie du Renseignement et des Services Secrets*, Paris: Lavauzelle, 1998.

———, *Encyclopédie des Terrorismes et Violences Politiques*, Panazol: Lavauzelle, 2003.

———, *Le Renseignement et la Lutte contre le Terrorisme: Stratégies et Perspectives Internationales*, Panazol: Lavauzelle, 2005.

Beevor, Antony, and Artemis Cooper, *Paris After the Liberation 1944–1949*, rev. ed., London: Penguin, 2004.

Bennett, Brian, and Douglas Waller, "Thwarting the Airline Plot: Inside the Investigation," *Time*, August 10, 2006. As of October 28, 2008: http://www.time.com/time/nation/article/0,8599,1225453,00.html

Bennett, Richard, *Espionage: An Encyclopedia of Spies and Secrets*, London: Virgin Books, 2002.

Bernard, Michel, *GIGN: Le Temps d'un Secret*, Paris: Bibliophane, 2003.

Bertin, François, *Gendarmerie Nationale: Des Prévots du Moyen Age au Gendarme de l'An 2000*, Rennes: Ouest-France, 1998.

Best, Richard A., *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, Washington, D.C.: Congressional Research Service, Library of Congress, January 16, 2001. As of October 10, 2008: http://gwis2.circ.gwu.edu/%7Egprice/crs.htm

Bétry, Alain, *L'EPIGN: L'Escadron Parachutiste d'Intervention de la Gendarmerie Nationale*, Atlante, 2001.

BfV—*see* Bundesamtes für Verfassungsschutz.

Bill C-36—*see* Parliament of Canada, House of Commons (2001).

BLAT—*see* Bureau de la Lutte Anti-terroriste.

Block, Ludo, "Evaluating the Effectiveness of French Counter-Terrorism," *Terrorism Monitor*, Vol. 3, No. 17, September 8, 2005. As of October 28, 2008: http://www.jamestown.org/terrorism/news/article.php?articleid=2369780

Bonner, Raymond, "Australian Court Rules for Indian," *New York Times*, August 22, 2007. As of October 23, 2008: http://www.nytimes.com/2007/08/22/world/asia/22australia.html

Boston, William, "The Intelligence Test," *Time*, April 25, 2004. As of October 28, 2008: http://www.time.com/time/magazine/article/0,9171,629319,00.html?iid=digg_share

Boukhars, Anouar, "The Threat of Islamist Terrorism to Germany," *Terrorism Monitor*, Vol. 5, No. 7, April 12, 2007, pp. 9–11. As of October 27, 2008: http://www.jamestown.org/terrorism/news/article.php?articleid=2373324

Boyes, Roger, "Algerians Jailed for Christmas Bomb Plot," *Times*, March 11, 2003. As of October 27, 2008: http://www.timesonline.co.uk/tol/news/world/article1118519.ece

———, "Train Bomb Plot Brings Fear of Terrorism to Germany," *Times*, August 21, 2006. As of October 27, 2008: http://www.timesonline.co.uk/tol/news/world/europe/article615030.ece

———, "Muslim Converts Target Germany," *Times*, September 6, 2007. As of October 27, 2008: http://www.timesonline.co.uk/tol/news/world/europe/article2390127.ece

Brook, Sir Norman, report, 1951, cited in Baron Alfred Denning, *The Denning Report: The Profumo Affair*, London: Pimlico, 1963, 1992 reprint.

Brown, Gordon, "Speech by the Rt. Hon. Gordon Brown MP, Chancellor of the Exchequer, at the Royal United Services Institute (RUSI), London," February 13, 2006. As of October 27, 2008: http://www.hm-treasury.gov.uk/1869.htm

———, "Statement on Security," July 25, 2007. As of October 27, 2008: http://www.number10.gov.uk/Page12675

Bundesamtes für Verfassungsschutz, "Islamism," Web page, undated(a). As of October 27, 2008: http://www.verfassungsschutz.de/en/en_fields_of_work/islamism/

———, "Scientology," Web page, undated(b). As of October 27, 2008: http://www.verfassungsschutz.de/en/en_fields_of_work/scientology/

———, *Controls of the Office for the Protection of the Constitution*, Köln, 2000.

———, *The Significance of Anti-Semitism in Current German Right-Wing Extremism*, Köln: Bundesministerium des Innern, 2002.

———, *Islamismus: Entstehung und aktuelle Erscheinungsformen*, Köln, 2006a.

———, *Verfassungsschutz gegen Rechtsextremismus*, Köln, 2006b.

———, *Office for the Protection of the Constitution: Tasks, Organization, and Working Methods*, Köln: Bundesministerium des Innern, 2007a.

———, *Integration as a Means to Prevent Extremism and Terrorism: Typology of Islamist Radicalisation and Recruitment*, Köln, January 2007b. As of October 27, 2008:
http://www.verfassungsschutz.de/download/SHOW/publication_0704_islamism_integration.pdf

———, *Der Verfassungsschutzbericht 2007*, May 15, 2008. As of October 27, 2008:
http://www.verfassungsschutz.de/de/publikationen/verfassungsschutzbericht/vsbericht_2007/

Burch, James, "A Domestic Intelligence Agency for the United States? A Comparative Analysis of Domestic Intelligence Agencies and Their Implications for Homeland Security," *Homeland Security Affairs*, Vol. 3, No. 2, June 2007, pp. 1–26. As of October 22, 2008:
http://www.hsaj.org/?article=3.2.2

Bureau de la Lutte Anti-terroriste, "La Gendarmerie dans la Lutte Antititerroriste," briefing, July 2005.

Cabinet Office, *Machinery of Government: Security and Counter-Terrorism, and the Criminal Justice System: Executive Summary*, March 2007. As of October 27, 2008:
http://www.attorneygeneral.gov.uk/attachments/Machinery%20of%20Government%20Changes,%20Security%20&%20Counter-Terrorism%20&%20the%20Criminal%20Justice%20System.pdf

———, "Intelligence and Security Committee," last updated October 21, 2008. As of October 27, 2008:
http://www.cabinetoffice.gov.uk/intelligence.aspx

Callinan, Rory, "Terror in the Suburbs?" *Time*, November 14, 2005. As of October 22, 2008:
http://www.time.com/time/magazine/article/0,9171,1130220,00.html?iid=chix-sphere

Campbell, A., "Trio Arrested Over Huge Terror Plot," *Metro*, September 6, 2007.

"Canadian Agencies Were Warned of Air India Attack in Advance," CBC News, April 30, 2007. As of October 23, 2008:
http://www.cbc.ca/canada/story/2007/04/29/airindia-inquiry.html

Canadian Security Intelligence Service, home page, undated. As of October 23, 2008:
http://www.csis-scrs.gc.ca/

———, *2002 Public Report*, Ottawa, Ont., c. 2002. As of October 23, 2008:
http://www.csis-scrs.gc.ca/pblctns/nnlrprt/2002/rprt2002-eng.asp

———, "Accountability and Review," Backgrounder No. 2, November 2004. As of October 23, 2008:
http://www.csis-scrs.gc.ca/nwsrm/bckgrndrs/bckgrndr02-eng.asp

———, *Public Report 2004–2005*, Ottawa, Ont., c. 2005a. As of October 23, 2008:
http://www.csis-scrs.gc.ca/pblctns/nnlrprt/2004/rprt2004-eng.asp

———, "The CSIS Mandate," Backgrounder No. 1, revised February 2005b. As of October 23, 2008:
http://www.csis-scrs.gc.ca/nwsrm/bckgrndrs/bckgrndr01-eng.asp

———, "Notes for Remarks to Carleton University Alumni Association, Rideau Club," May 24, 2007a. As of January 9, 2009:
http://www.csis-scrs.gc.ca/nwsrm/spchs/spch24052007-eng.asp

———, "Counter-Terrorism," Backgrounder No. 8, revised June 2007b. As of October 23, 2008:
http://www.csis-scrs.gc.ca/nwsrm/bckgrndrs/bckgrndr08-eng.asp

"Le Cauchemar de l'Airbus Alger-Paris," *Paris Match*, Vol. 2380, January 5, 1995.

Centre for the Protection of National Infrastructure, "About CPNI," Web page, undated. As of October 27, 2008:
http://www.cpni.gov.uk/about.aspx

Cettina, Natahalie, "The French Approach: Vigour and Vigilance," in Marianne van Leeuwen, ed., *Confronting Terrorism: European Experiences, Threat Perceptions and Policies*, The Hague and Boston, Mass.: Kluwer Law International, 2003.

Chalk, Peter, *Australian Foreign and Defense Policy in the Wake of the 1999/2000 East Timor Intervention*, Santa Monica, Calif.: RAND Corporation, MR-1409-SRF, 2001. As of October 22, 2008:
http://www.rand.org/pubs/monograph_reports/MR1409/

———, "Militant Islamic Extremism in Southeast Asia," in Paul J. Smith, ed., *Terrorism and Violence in Southeast Asia: Transnational Challenges to States and Regional Stability*, Armonk, N.Y.: M. E. Sharpe, 2005.

Chalk, Peter, and William Rosenau, *Confronting "the Enemy Within": Security Intelligence, the Police, and Counterterrorism in Four Democracies*, Santa Monica, Calif.: RAND Corporation, MG-100-RC, 2004. As of October 10, 2008: http://www.rand.org/pubs/monographs/MG100/

Choquet, Christian, "La Structure Administrative des Services de Renseignement," in Bertrand Warusfel, ed., *Le Renseignement Français Contemporain: Aspects Politiques et Juridiques*, Paris: Harmattan, 2003.

Clarke, Peter, Deputy Assistant Commissioner, Counter Terrorism Command, Scotland Yard, *Learning from Experience: Counter Terrorism in the UK Since 9/11*, Colin Cramphorn Memorial Lecture, April 24, 2007. As of October 27, 2008: http://www.policyexchange.org.uk/images/libimages/252.pdf

Cleaver, Hannah, "Germany's Top Neo-Nazis Spy for Ministry," *Telegraph*, July 16, 2002a.

———, "September 11 'Bank Manager' Is Charged," *Telegraph*, August 29, 2002b. As of October 27, 2008: http://www.telegraph.co.uk/news/worldnews/europe/germany/1405716/September-11-bank-manager-is-charged.html

Clutterbuck, Lindsay, "Countering Irish Republican Terrorism in Britain: Its Origin as a Police Function," *Terrorism and Political Violence*, Vol. 18, No. 1, Spring 2006, pp. 95–118.

Clutterbuck, Richard L., *Britain in Agony: The Growth of Political Violence*, London and Boston: Faber and Faber, 1978.

Cobain, Ian, "Torture: MPs Call for Inquiry into MI5 Role," *Guardian*, July 15, 2008a. As of October 28, 2008: http://www.guardian.co.uk/world/2008/jul/15/humanrights.civilliberties

———, "Watchdog Asked to Investigate Pakistan Torture Allegation," *Guardian*, July 16, 2008b. As of October 28, 2008: http://www.guardian.co.uk/world/2008/jul/16/humanrights.terrorism

Combelles Siegel, Pascale, "An Inside Look at France's Mosque Surveillance Program," *Terrorism Monitor*, Vol. 5, No. 16, August 16, 2007. As of October 28, 2008: http://www.jamestown.org/terrorism/news/article.php?articleid=2373621

Combs, Cindy C., *Terrorism in the Twenty-First Century*, 4th ed., Upper Saddle River, N.J.: Pearson/Prentice Hall, 2006.

Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar*, Ottawa, 2006.

Connolly, Kate, "Islamic Extremists Jailed for Bomb Plot," *Telegraph*, March 10, 2003. As of October 27, 2008:

http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/1424313/Islamic-extremists-jailed-for-bomb-plot.html

Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe. As of October 27, 2008: http://conventions.coe.int/

"Counter-Terrorism," House of Commons Debate, Vol. 207, May 8, 1992, columns 296–306.

"Couple Wins Payout Over ASIO, AFP Raid," ABC News Online, November 1, 2005. As of October 23, 2008: http://www.abc.net.au/news/newsitems/200511/s1495493.htm

Courtois, Jean-Louis, *Le Raid, l'Unité d'Élite de la Police Française*, Paris: Pygmalion, 1999.

Cowell, Alan, and Raymond Bonner, "In Hunt for Bomb Plotters, Britain Sees a Qaeda Link," *New York Times*, July 2, 2007. As of October 23, 2008: http://www.nytimes.com/2007/07/02/world/europe/02britain.html

CPNI—*see* Centre for the Protection of National Infrastructure.

CSIS—*see* Canadian Security Intelligence Service.

Dard, Olivier, "L'OAS: Histoire d'un Refus," *Guerre d'Algérie*, Vol. 8, June–July–August 2007.

Dartnell, Michael York, *Action Directe: Ultra-Left Terrorism in France, 1979–1987*, London and Portland, Oreg.: Frank Cass, 1995.

Delaporte, Ixchel, "L'Exportation de la Torture," *L'Humanité*, August 30, 2003. As of October 24, 2008: http://www.humanite.fr/2003-08-30_Medias_-L-exportation-de-la-torture

Department of the Prime Minister and Cabinet, *Protecting Australia Against Terrorism 2006: Australia's National Counter-Terrorism Policy and Arrangements*, Barton, ACT, 2006. As of October 22, 2008: http://www.dpmc.gov.au/publications/protecting_australia_2006/docs/paat_2006.pdf

DeRosa, Mary, *Data Mining and Data Analysis for Counterterrorism*, Washington, D.C.: CSIS Press, 2004.

DGPN—*see* Direction Générale de la Police Nationale.

DHS OIG—*see* U.S. Department of Homeland Security Office of the Inspector General.

Dietl, Wilhelm, Kai Hirschmann, and Rolf Tophoven, *Das Terrorismus-Lexikon: Täter, Opfer, Hintergründe*, Frankfurt am Main: Eichborn, 2006.

Direction Générale de la Police Nationale, *Counter Terrorism Coordination Unit: Unite de Coordination de la Lutte Anti-Terroriste (UCLAT)*, Paris: DGPN/UCLAT, June 2003.

Direction Générale de la Police Nationale, Unité de Recherche, d'Assistance, d'Intervention, et de Dissuasion, *Le Raid, l'Unité d'Élite de la Police Française*, Chaumont: Editions Crépin-Leblond, 2005.

Dobson, Christopher, and Ronald Payne, *The Carlos Complex: A Pattern of Violence*, London: Hodder and Stoughton, 1977.

Dyer, Clare, "Lords Back Terror Law Orders on Suspects, but Give Them New Rights," *Guardian*, November 1, 2007. As of October 27, 2008: http://www.guardian.co.uk/uk/2007/nov/01/terrorism.law

ECHR—*see* Convention for the Protection of Human Rights and Fundamental Freedoms.

European Commission for Democracy Through Law, *Report on the Democratic Oversight of the Security Services*, adopted by the Venice Commission at its 71st Plenary Session, Venice, June 1–2, 2007. As of October 27, 2008: http://www.venice.coe.int/docs/2007/CDL-AD(2007)016-e.asp

Evans, Jonathan, director general of the security service, "Conviction of Fertiliser Plotters," Security Service, April 2007a. As of October 27, 2008: http://www.mi5.gov.uk/output/Page383.html

———, "Links Between the 7 July Bombers and the Fertiliser Plotters," Security Service, April 2007b. As of October 27, 2008: http://www.mi5.gov.uk/output/Page384.html

———, "Intelligence, Counter-Terrorism and Trust," address to the Society of Editors' "A Matter of Trust" conference, Manchester, UK, November 5, 2007c. As of October 27, 2008: http://www.mi5.gov.uk/output/Page562.html

Fairchild, Erika S., and Harry R. Dammer, *Comparative Criminal Justice Systems*, 2nd ed., Belmont, Calif.: Wadsworth/Thomson Learning, 2001.

Faligot, Roger, "L'Affaire Topaze: Foccart Est un Agent du KGB," in Roger Faligot, Jean Guisnel, and Rémi Kauffer, eds., *Histoire Secrète de la Ve République*, Paris: La Découverte, 2006a, pp. 394–399.

———, "La France Complice ou Otage de la Seconde Guerre d'Algérie?" in Roger Faligot, Jean Guisnel, and Rémi Kauffer, eds., *Histoire Secrète de la Ve République*, Paris: La Découverte, 2006b, pp. 447–459.

———, "Les Services Secrets Français dans la Guerre Froide," in Roger Faligot, Jean Guisnel, and Rémi Kauffer, eds., *Histoire Secrète de la Ve Républiqu*e, Paris: La Découverte, 2006c.

Faligot, Roger, and Pascal Krop, *DST: Police Secrète*, Paris: Flammarion, 1999.

Fall, Bernard B., *Hell in a Very Small Place: The Siege of Dien Bien Phu*, New York: Da Capo Press, 1985.

———, *Street Without Joy: The French Debacle in Indochina*, Barnsley: Pen and Sword Military, 2005.

Farrugia, Emmanuel, and Paul Serf, *Corse: Le terrorisme*, Paris: DIE, 2004.

Faure, Claude, *Aux Services de la République: Du BCRA à la DGSE*, Paris: Fayard, 2004.

Finn, Peter, "Hamburg's Cauldron of Terror," *Washington Post*, September 11, 2002, p. A01. As of October 28, 2008:
http://www.washingtonpost.com/wp-dyn/articles/A64793-2002Sep10.html

"Five Get Life over UK Bomb Plot," BBC News, April 30, 2007. As of October 27, 2008:
http://news.bbc.co.uk/2/hi/uk_news/6195914.stm

Follorou, Jacques, and Vincent Nouzille, *Les Parrains Corses*, Paris: Fayard, 2004.

Friscolanti, Michael, Jonathon Gatehouse, and Charlie Gillis, "Homegrown Terror: It's Not Over," *Macleans*, June 19, 2006. As of October 28, 2008:
http://www.macleans.ca/canada/national/article.jsp?content=20060619_128953_128953

Fyfe, Sir David Maxwell, directive, September 24, 1952, in Baron Alfred Denning, *The Denning Report: The Profumo Affair*, London: Pimlico, 1963, 1992 reprint.

Gabor, Thomas, ed., *The Views of Canadian Scholars on the Impact of the Anti-Terrorism Act*, draft final report, March 31, 2004. As of October 28, 2008:
http://www.justice.gc.ca/eng/pi/rs/rep-rap/2005/rr05_1/

GAO—*see* U.S. General Accounting Office.

Gerecht, Reuel Marc, and Gary J. Schmitt, "What France Does Best," *American*, March–April 2008. As of October 28, 2008:
http://www.american.com/archive/2008/march-april-magazine-contents/what-france-does-best

"German Intelligence Must Stop Computer Spying, Lawmakers Say," *Deutsche Welle*, April 26, 2007. As of October 27, 2008:
http://www.dw-world.de/dw/article/0,2144,2458692,00.html

"Germany to Revamp Domestic Intelligence Service," *Deutsche Welle*, March 18, 2004. As of October 28, 2008:
http://www.dw-world.de/dw/article/0,2144,1145132,00.html

Gilmore Commission—*see* Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction.

Gomart, Thomas, "Les Services de Renseignement Français face à la Menace Soviétique au début des Années Soixante (1958–1964)," in Bertrand Warusfel, ed., *Le Renseignement: Guerre, Technique et Politique (XIXe–XXe Siècles)*, Panazol: Lavauzelle, 2007.

Gozzi, Marie-Hélène, *Le Terrorisme*, Paris: Ellipses, 2003.

Gregory, Frank, "Intelligence-Led Counter-Terrorism: A Brief Analysis of the UK Domestic Intelligence System's Response to 9/11 and the Implications of the London Bombings of 7 July 2005," *Real Instituto Elcano*, Analysis of the Real Institute 94/2005, July 12, 2005. As of October 28, 2008: http://www.realinstitutoelcano.org/analisis/781/Gregory781-v.pdf

———, "A Critical Analysis of Recent Developments in UK Counter-Terrorism Policies and the Implications of the Car Bomb Incidents of June 2007," *Real Instituto Elcano*, Analysis of the Real Institute 115/2007, October 29, 2007. As of October 27, 2008: http://www.realinstitutoelcano.org/wps/portal/rielcano_in/Content?WCM_GLOBAL_CONTEXT=/Elcano_in/Zonas_in/ARI115-2007

———, "The Police and Intelligence Services: With Special Reference to the Police/MI5 Relationship," in Clive Harfield, John Grieve, Allyson MacVean, and David Phillips, eds., *The Handbook of Intelligent Policing: Consilience, Crime Control, and Community Safety*, Oxford and New York: Oxford University Press, 2008, pp. 47–62.

Grono, Nicholas, "Australia's Response to Terrorism," *Studies in Intelligence*, Vol. 48, No. 1, 2004. As of October 22, 2008: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no1/article03.html

Gunaratna, Rohan, *Inside al Qaeda: Global Network of Terror*, 2nd ed., London: Hurst and Company, 2003.

Hamon, Alain, and Jean Charles Marchand, *Action Directe, du Terrorisme Française à l'Euroterrorisme*, Paris: Editions de Seuil/L'Epreuve des Faits, 1986.

Harclerode, Peter, *Secret Soldiers: Special Forces in the War Against Terrorism*, London: Cassell, 2000.

Hardaker, David, "ASIO Targeted as Back Door to US Intelligence," *PM*, November 1, 2004. As of June 15, 2007: http://www.abc.net.au/pm/content/2004/s1232375.htm

Harfield, Clive, and Karen Harfield, *Covert Investigation*, Oxford and New York: Oxford University Press, 2005.

Haynes, Alan, *Invisible Power: The Elizabethan Secret Services, 1570–1603*, Stroud: A. Sutton, 1992.

Head, Mike, "Australian Federal Police Commissioner Reveals Scale of Haneef Frame-Up," *World Socialist Web Site*, March 3, 2008a. As of July 14, 2008: http://www.wsws.org/articles/2008/mar2008/afp-m03.shtml

———, "Australia: Haneef Inquiry Seeks to 'Restore Confidence' in Terror Laws," *World Socialist Web Site*, March 26, 2008b. As of July 14, 2008: http://www.wsws.org/articles/2008/mar2008/hane-m26.shtml

Helm, T., "Germans Foil al-Qaeda Plot to Bomb US Base," *Telegraph*, September 7, 2002.

Her Majesty's Stationery Office, *Report from the Select Committee on the Petition of Frederick Young and Others (Police)*, London, 1833.

———, *National Intelligence Machinery*, September 2006. As of October 27, 2008: http://www.intelligence.gov.uk/~/media/assets/www.intelligence.gov.uk/national_intelligence_booklet%20pdf.ashx

Hinsliff, Gaby, "PM Offers Pact to Stop Pakistan Exporting Terror," *The Gaurdian* (London), December 15, 2008.

HMSO—*see* Her Majesty's Stationery Office.

Home Office, Scottish Executive, and Northern Ireland Office, *Guidelines on Special Branch Work in the United Kingdom*, London: Home Office Communication Directorate, 2004. As of October 27, 2008: http://www.scotland.gov.uk/library5/justice/sbwuk.pdf

Homeland Security Council, and President George W. Bush, *National Strategy for Homeland Security*, Washington, D.C.: The White House, October 2007. As of October 28, 2008: http://purl.access.gpo.gov/GPO/LPS88800

Horchem, Hans Josef, "Terrorism and Government Response: The German Experience," in Edward Moxon-Browne, ed., *European Terrorism*, Aldershot: Dartmouth, 1993.

———, "The Terrorist Lobby in West Germany: Campaigns and Propaganda in Support of Terrorism," in No'omi Gal-Or, ed., *Tolerating Terrorism in the West: An International Survey*, London: Routledge, 1991.

Horne, Alistair, *A Savage War of Peace: Algeria 1954–1962*, London: Papermac, 1996.

Human Rights Act 1998 (c. 42). As of October 27, 2008: http://www.opsi.gov.uk/ACTS/acts1998/ukpga_19980042_en_1

ICG—*see* International Crisis Group.

Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, May 2006.

Intelligence Services Act 1994 (c. 13). As of October 27, 2008: http://www.opsi.gov.uk/ACTS/acts1994/ukpga_19940013_en_1

International Crisis Group, *Jemaah Islamiyah in South East Asia, Damaged but Still Dangerous*, Jakarta and Brussels, Asia report 63, August 26, 2003. As of October 22, 2008: http://www.crisisgroup.org/home/getfile.cfm?id=132&tid=1452&type=pdf&l=1

———, *Indonesia: Jemaah Islamiyah's Current Status*, Jakarta and Brussels, Asia briefing 63, May 3, 2007. As of October 22, 2008: http://www.crisisgroup.org/library/documents/asia/indonesia/b63_indonesia_jemaah_islamiyah_s_current_status.pdf

Investigatory Powers Tribunal, "Additional Oversight," last updated May 5, 2006. As of October 27, 2008: http://www.ipt-uk.com/default.asp?sectionID=8

IPT—*see* Investigatory Powers Tribunal.

"Is Germany Next on the Terrorists' List?" *Week*, April 27, 2002.

Jackson, Brian A., *The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency*, Santa Monica, Calif.: RAND Corporation, MG-804-DHS, 2009.

Jackson, Brian A., Peter Chalk, Kim Cragin, Bruce Newsome, John V. Parachini, William Rosenau, Erin M. Simpson, Melanie Sisson, and Donald Temple, *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*, Santa Monica, Calif.: RAND Corporation, MG-481-DHS, 2007. As of October 10, 2008: http://www.rand.org/pubs/monographs/MG481/

Jackson, James O., "Death on Track 4," *Time*, August 23, 1993. As of October 27, 2008: http://www.time.com/time/magazine/article/0,9171,979072,00.html

Jiwa, Salim, *The Death of Air India Flight 182*, London: W. H. Allen, 1987.

Johnson, Matthew M., "FBI's Intelligence Woes Restir Debate on an American MI5," *CQ Homeland Security*, October 23, 2007.

Johnston, Tim, "Australian Judge Dismisses Terrorism Case," *New York Times*, November 13, 2007. As of October 23, 2008: http://www.nytimes.com/2007/11/13/world/asia/13australia.html?ex=1352610000&en=f77331cefcf2e3ef&ei=5088&partner=rssnyt&emc=rss

Jordan, Mary, "Britain's MI5 Warns of Rising Terror Threat," *Washington Post*, November 11, 2006, p. A15. As of October 28, 2008: http://www.washingtonpost.com/wp-dyn/content/article/2006/11/10/AR2006111000138.html

"Judge Critical of MI5 Testimony," BBC News, October 12, 2006. As of October 28, 2008:
http://news.bbc.co.uk/2/hi/uk_news/6042872.stm

Kaiser, Simone, Marcel Rosenbach, and Holger Stark, "Operation Alberich: How the CIA Helped Germany Foil Terror Plot," *Spiegel*, September 10, 2007. As of October 28, 2008:
http://www.spiegel.de/international/germany/0,1518,504837,00.html

Karacs, Imre, "Germany Uses New Law to Ban Muslim Group," *Independent*, December 13, 2001. As of October 27, 2008:
http://www.independent.co.uk/news/world/europe/germany-uses-new-law-to-ban-muslim-group-620064.html

Karmon, Ely, "German and Palestinian Terrorist Organizations: Strange Bedfellows—An Examination of the Coalitions Among Terrorist Organizations," May 10, 2000. As of October 27, 2008:
http://212.150.54.123/articles/articledet.cfm?articleid=120

Katz, Rita, and Michael Kern, "Terrorist 007, Exposed," *Washington Post*, March 26, 2006, p. B01. As of October 28, 2008:
http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500020.html

Kauffer, Rémi, "La 'Gangrène de la Gégène,' ou la Torture en Algérie," in Roger Faligot, Jean Guisnel, and Rémi Kauffer, eds., *Histoire Secrète de la Ve République*, Paris: La Découverte, 2006a, pp. 35–44.

———, "Les Soldats Perdus de l'OAS," in Roger Faligot, Jean Guisnel, and Rémi Kauffer, eds., *Histoire Secrète de la Ve République*, Paris: La Découverte, 2006b.

———, "La Véritable Histoire des 'Barbouzes Gaullistes,'" in Roger Faligot, Jean Guisnel, and Rémi Kauffer, eds., *Histoire Secrète de la Ve République*, Paris: La Découverte, 2006c.

Kepel, Gilles, *Jihad: The Trail of Political Islam*, London: I. B. Tauris, 2003.

King, David, "Protest Over Delay for Terror Suspects," *Australian*, January 15, 2006.

Klausen, Jytte, "British Counter-Terrorism After the July 2005 Attacks: Adapting Community-Policing to the Fight Against Domestic Terrorism," USIPeace Briefing, February 2007.

Lander, Sir Stephen, Director General of the Security Service, "British Intelligence in the 21st Century," transcript of the lecture to the Public Records Office Conference, "The Missing Dimension," June 21, 2001. As of October 27, 2008:
http://www.mi5.gov.uk/output/Page379.html

Landler, Mark, and Nicholas Kulish, "Turkish Connection Shakes Germans," *International Herald Tribune*, September 8, 2007.

Le Page, J. M., "Les Services de Renseignements Français à Dien Bien Phu," in Bertrand Warusfel, ed., *Le Renseignement: Guerre, Technique et Politique (XIXe–XXe Siècles)*, Panazol: Lavauzelle, 2007.

Lewis, Jason, "Terror Plot Suspects Bugged by MI5 'Sneak and Peak' Teams," *Daily Mail*, August 12, 2006. As of October 28, 2008: http://www.dailymail.co.uk/news/article-400310/Terror-plot-suspects-bugged-MI5-sneak-peak-teams.html

Lichfield, John, "Sarkozy Makes Bid to Take Personal Charge of the Secret Services," *Independent*, June 29, 2007. As of October 24, 2008: http://www.independent.co.uk/news/world/europe/sarkozy-makes-bid-to-take-personal-charge-of-the-secret-services-455190.html

MacCharles, Tonda, "Day Seeks Security Powers," *Toronto Star*, May 16, 2007. As of October 28, 2008: http://www.thestar.com/News/article/214387

Madden, James, and Simon Kearney, "Rockets to Be Fired in Terror Plot," *Australian*, January 6, 2007. As of October 28, 2008: http://www.theaustralian.news.com.au/story/0,20867,21017915-601,00.html

Mahon, Claire, and Karyn Palmer, "How the ASIO Bill Ravages Your Civil Rights," *Age*, June 23, 2003. As of October 28, 2008: http://www.theage.com.au/articles/2003/06/22/1056220477057.html

Maley, Paul, "Not Enough Haneef Evidence, AFP Told," *Australian*, July 10, 2008. As of October 23, 2008: http://www.theaustralian.news.com.au/story/0,,23998084-2702,00.html

Manningham-Buller, Dame Eliza, director general of the Security Service, *Global Terrorism: Are We Meeting the Challenge*, James Smart lecture, City of London Police Headquarters, October 16, 2003.

Markle Foundation Task Force, *Protecting America's Freedom in the Information Age*, New York and Washington, D.C.: Markle Foundation, October 2002. As of October 10, 2008: http://www.markletaskforce.org/documents/Markle%5FFull%5FReport.pdf

Masse, Todd, *Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States*, Washington, D.C.: Library of Congress, Congressional Research Service, 03-RL-31920, May 19, 2003. As of October 10, 2008: http://handle.dtic.mil/100.2/ADA455815

———, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, Washington, D.C.: Library of Congress, Congressional Research Service, RL33616, August 18, 2006. As of October 10, 2008: http://handle.dtic.mil/100.2/ADA454484

McAllister, Richard, "Support from a Bicephalous Executive: France," in Mary Buckley and Rick Fawn, eds., *Global Responses to Terrorism: 9/11, Afghanistan, and Beyond*, London and New York: Routledge, 2003, pp. 90–100.

McGregor, Glen, "Court Ruling Highlights Need to Give CSIS More Power, Expert Says," *Ottawa Citizen*, February 16, 2008. As of October 28, 2008: http://www.canada.com/ottawacitizen/news/story.html?id=265f3a15-b1ab-4963-9e2a-2ac08480769a&k=40597

McHugh, D., "Germany: Terror Threat Is on the Rise," *Guardian*, June 22, 2007.

McKnight, David, *Australia's Spies and Their Secrets*, St. Leonards, NSW, Australia: Allen and Unwin, 1994.

McNulty, Tony, Home Office minister for the police, radio interview, *Today*, BBC Radio 4, October 1, 2007.

Merlen, Eric, and Frédéric Ploquin, *Carnets Intimes de la DST: 30 Ans au Coeur du Contre Espionnage Français*, Paris: Fayard, 2003.

Metropolitan Police Act of 1829, 10 Geo. 4, c. 44.

Metropolitan Police Service, *Metropolitan Police Instruction Book*, London, 1829.

Meyer, Eitan, "The Bundesgrenzschutz German Federal Border Guard and Protector of German Internal Security," *Intersec*, Vol. 11, No. 7–8, July–August 2001, pp. 234–237.

MI5—*see* Security Service.

"MI5 Followed UK Suicide Bomber," BBC News, April 30, 2007. As of October 27, 2008: http://news.bbc.co.uk/2/hi/uk_news/6417353.stm

Micheletti, Eric, *Le GIGN en Action*, Paris: Histoire and Collections, 1997.

———, *Special Forces in Afghanistan: 2001–2003: War Against Terrorism*, Paris: Histoire and Collections, 2003.

Miko, Francis T., and Christian Froehlich, *Germany's Role in Fighting Terrorism: Implications for U.S. Policy*, Washington, D.C.: Congressional Research Service, Library of Congress, RL32710, December 27, 2004. As of October 27, 2008: http://handle.dtic.mil/100.2/ADA444776

Milligan, Darric, Bernadette Clemente, and Michael Schader, *Intelligence-Led Policing Tool: Intelligence-Led Policing Technology for State and Local Law Enforcement Agencies*, Falls Church, Va.: Mitretek Systems and Yellow House Associates, MTR-2006-016, March 2006. As of October 10, 2008: http://www.noblis.org/BusinessAreas/CriminalJustice/ILPT_MTR-2006-016.pdf

Ministère de l'Interieur, de l'Outre-mer, et des Collectivités Territoriales, "*La Police Nationale: La Direction Centrale des Renseignements Généraux*," last modified July 17, 2006. As of October 23, 2008:

http://www.interieur.gouv.fr/sections/a_l_interieur/la_police_nationale/organisation/dcrg/dcrg/view

Ministry of Home Affairs, *The Jemaah Islamiyah Arrests and the Threat of Terrorism: White Paper*, Singapore, January 7, 2003.

"La Mission," *VSD*, December 29, 1994.

Morgan, Richard E., *Domestic Intelligence: Monitoring Dissent in America*, Austin, Tex.: University of Texas Press, 1980.

NAA—*see* National Archives of Australia.

NAO—*see* National Audit Office.

National Archives of Australia, "Fact Sheet 130: The Royal Commission on Espionage, 1954–55," updated December 2006. As of October 23, 2008: http://www.naa.gov.au/about-us/publications/fact-sheets/fs130.aspx

National Audit Office, home page, undated. As of October 27, 2008: http://www.nao.org.uk/

———, *Thames House and Vauxhall Cross: Report*, London: Stationery Office, 2000.

National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*, New York: Norton, 2004.

National Security Agency, "Signals Intelligence: Who Is Considered a U.S. Person?" Web page, undated. As of October 10, 2008: http://www.nsa.gov/about/about00020.cfm#5

"'No Need' for New MI5 Base in NI," BBC News, October 23, 2006. As of October 27, 2008: http://news.bbc.co.uk/1/hi/northern_ireland/6078578.stm

Norton-Taylor, Richard, "MI5 to Expand Regional Offices," *Guardian*, November 8, 2005. As of October 27, 2008: http://www.guardian.co.uk/politics/2005/nov/08/terrorism.uksecurity

NSA—*see* National Security Agency.

O'Brien, Natalie, "Is This Man the Hilton Bomber?" *Weekend Australian*, February 8–9, 2003.

Office of Homeland Security, *National Strategy for Homeland Security*, Washington, D.C., July 2002. As of October 10, 2008: http://purl.access.gpo.gov/GPO/LPS20641

Parker, John, *Inside the Foreign Legion: The Sensational Story of the World's Toughest Army*, London: Piatkus, 1998.

Parliament of Canada, House of Commons, Anti-Terrorism Act, Bill C-36, December 18, 2001. As of October 28, 2008: http://www2.parl.gc.ca/HousePublications/Publication.aspx?pub=bill&doc=c-36&parl=37&ses=1&language=E&File=16

Parliament of the Commonwealth of Australia, House of Representatives, Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002: A Bill for an Act to Amend Legislation Relating to the Australian Security Intelligence Organisation to Enhance the Commonwealth's Ability to Combat Terrorism, and for Related Purposes, 2003. As of October 28, 2008: http://parlinfoweb.aph.gov.au/piweb/Repository/Legis/Bills/Linked/17040301.pdf

———, Anti-Terrorism Bill (No. 2) 2004: A Bill for an Act Relating to Foreign Travel Documents, Persons in Relation to Whom ASIO Questioning Warrants Are Being Sought, Associating with Terrorist Organisations, the Transfer of Prisoners, Forensic Procedures, and for Other Purposes, 2004. As of October 28, 2008: http://www.comlaw.gov.au/ComLaw/Legislation/Bills1.nsf/framelodgmentattachments/783512FE01F443CCCA256F7200262327

Parliamentary Joint Committee on ASIO, ASIS, and DSD, *An Advisory Report on the Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002*, Canberra, May 2002.

Parmentier, Guillaume, "France," in Yonah Alexander, ed., *Counterterrorism Strategies: Successes and Failures of Six Nations*, Washington, D.C.: Potomac Books, 2006, pp. 44–71.

Paterson, T., "Despair Over Fate of Sahara Tourists," *Telegraph*, April 20, 2003. As of October 27, 2008: http://www.telegraph.co.uk/news/worldnews/europe/austria/1428025/Despair-over-fate-of-Sahara-tourists.html

Perry, Michael, "Sydney Nuclear Reactor Terror Plot Target–Police," (Reuters) *Washington Post*, November 14, 2005. As of October 28, 2008: http://www.washingtonpost.com/wp-dyn/content/article/2005/11/14/AR2005111400036.html

Peters, Butz, *Tödlicher Irrtum: die Geschichte der RAF*, Berlin, Argon, 2004.

Peterson, Marilyn B., *New Realities: The New Intelligence Architecture/Intelligence-Led Policing*, Washington, D.C.: U.S. Dept. of Justice, Office of Justice Programs, Bureau of Justice Assistance, September 2005. As of October 21, 2008: http://purl.access.gpo.gov/GPO/LPS64949

Petter, Nick, "Turkish Diplomat Survived 1985 Embassy Siege: Ambassador Hurled Himself Out Window During Attack," *Ottawa Citizen*, March 7, 2005.

Pluchinsky, Dennis A., "Germany's Red Army Faction: An Obituary," *Studies in Conflict and Terrorism*, Vol. 16, No. 2, 1993, pp. 135–157.

PM&C—*see* Department of the Prime Minister and Cabinet.

"Police Had Hint 11 Days Before 1985 Air India Bombing, Inquiry Hears," CBC News, May 1, 2007. As of October 23, 2008:
http://www.cbc.ca/canada/story/2007/05/01/air-india.html

Porch, Douglas, *The French Foreign Legion: A Complete History*, London: Macmillan, 1993.

———, *The French Secret Services: From the Dreyfus Affair to the Gulf War*, Oxford and New York: Oxford University Press, 1997.

Porter, Bernard, *The Origins of the Vigilant State: The London Metropolitan Police Special Branch Before the First World War*, London: Weidenfeld and Nicolson, 1987.

Premier Ministre, *Prevailing Against Terrorism: White Paper on Domestic Security Against Terrorism*, Paris: Documentation française, 2006. As of October 28, 2008:
http://www.ambafrance-dk.org/IMG/pdf/livre_blanc_english.pdf

"Preventing Terrorism Together" Working Groups, August–October 2005. As of October 28, 2008:
http://www.communities.gov.uk/documents/communities/pdf/152164.pdf

"*Les Principaux Services du Ministère de l'Intérieur Exerçant des Missions de Renseignement*," La Documentation Française, Web page, undated. As of October 24, 2008:
http://www.ladocumentationfrancaise.fr/dossiers/renseignement-terrorisme/ministere-interieur.shtml

Public Safety Canada, home page, undated. As of October 23, 2008:
http://www.ps-sp.gc.ca/

Rabasa, Angel, Peter Chalk, Kim Cragin, Sara A. Daly, Heather S. Gregg, Theodore W. Karasik, Kevin A. O'Brien, and William Rosenau, *Beyond al-Qaeda*, Part 1: *The Global Jihadist Movement*, Santa Monica, Calif.: RAND Corporation, MG-429-AF, 2006. As of October 22, 2008:
http://www.rand.org/pubs/monographs/MG429/

Ratcliffe, J., "Intelligence-Led Policing and the Problems of Turning Rhetoric into Practice," *Policing and Society*, Vol. 12, No. 1, January 2002, pp. 53–66.

Rayment, Sean, "Security Forces 'Foil Terror Plot Every Six Weeks,'" *Telegraph*, February 5, 2007. As of October 28, 2008:
http://www.telegraph.co.uk/news/uknews/1541543/Security-forces-foil-terror-plot-every-six-weeks.html

RCASIA—*see* Royal Commission on Australia's Security and Intelligence Agencies.

Reeve, Simon, *One Day in September: The Full Story of the 1972 Munich Olympics Massacre and the Israeli Revenge Operation "Wrath of God," with a New Epilogue*, New York: Arcade, 2006.

Regulation of Investigatory Powers Act 2000 (c. 23). As of October 27, 2008: http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1

Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism, SOR/2001-360, October 2, 2001. As of October 23, 2008: http://laws.justice.gc.ca/en/ShowDoc/cr/SOR-2001-360/bo-ga:s_1::bo-ga:s_2/20081023/en

Revised Statutes of Canada, ch. C-23, Canadian Security Intelligence Service Act (1985).

Riley, K. Jack, Gregory F. Treverton, Jeremy M. Wilson, and Lois M. Davis, *State and Local Intelligence in the War on Terrorism*, Santa Monica, Calif.: RAND Corporation, MG-394-RC, 2005. As of October 10, 2008: http://www.rand.org/pubs/monographs/MG394/

Rimington, Stella, *Open Secret: The Autobiography of the Former Director-General of MI5*, London: Hutchinson, 2001.

Rodier, Alain, *Al-Qaida: Les Connexions Mondiales du Terrorisme*, Paris: Ellipses, 2006.

Rojahn, Christoph, *Left-Wing Terrorism in Germany: The Aftermath of Ideological Violence*, Warwickshire: Research Institute for the Study of Conflict and Terrorism, 1998.

Royal Commission on Australia's Security and Intelligence Agencies, *Report on the Australian Security Intelligence Organisation*, Canberra: Australian Government Publishing Service, 1985.

Schanzer, Jonathan, *Al-Qaeda's Armies: Middle East Affiliate Groups, Ungoverned Territories and the Next Generation of Terror*, New York: SPI, 2004.

Schmidt, Michael, *New Reich: Penetrating the Secrets of Today's Neo-Nazi Networks*, London: Hutchinson, 1993.

Sciolino, Elaine, "French, Seeing Terror Plot, Arrest 20 During Raids in Paris Region, *New York Times*, December 13, 2005. As of October 28, 2008: http://www.nytimes.com/2005/12/13/international/europe/13france.html?partner=rssnyt&emc=rss

———, "France's Terrorism Strategy Faulted," *New York Times*, July 3, 2008. As of October 28, 2008: http://www.nytimes.com/2008/07/03/world/europe/03france.html?emc=rss&partner=rssnyt

"Secrets of the Thatcher Years May Be Revealed a Decade Early," *Times*, October 26, 2007, pp. 30–31.

"Security and Intelligence 2007 Pre-Budget Report," press release, Home Office Press Office, October 10, 2007. As of October 27, 2008: http://press.homeoffice.gov.uk/press-releases/security-prebudget-report

Security Intelligence Review Committee, *The Heritage Front Affair: Report to the Solicitor General of Canada*, December 9, 1994.

———, *SIRC Annual Report 2003–2004: An Operational Review of the Canadian Security Intelligence Service*, Ottawa, Ont., September 30, 2004. As of October 23, 2008: http://www.sirc-csars.gc.ca/anrran/2003-2004/index-eng.html

———, *SIRC Annual Report 2005–2006: An Operational Review of the Canadian Security Intelligence Service*, Ottawa, Ont., September 29, 2006. As of October 23, 2008: http://www.sirc-csars.gc.ca/anrran/2005-2006/index-eng.html

———, *SIRC Annual Report 2006–2007: An Operational Review of the Canadian Security Intelligence Service*, Ottawa, Ont., September 28, 2007. As of October 23, 2008: http://www.sirc-csars.gc.ca/anrran/2006-2007/index-eng.html

Security Service, "About Us," Web page, undated(a). As of October 27, 2008: http://www.mi5.gov.uk/output/Page15.html

———, "Gathering Intelligence," Web page, undated(b). As of October 27, 2008: http://www.mi5.gov.uk/output/Page71.html

———, "How We Operate," Web page, undated(c). As of October 27, 2008: http://www.mi5.gov.uk/output/Page55.html

———, "Joint Terrorism Analysis Centre," Web page, undated(d). As of October 27, 2008: http://www.mi5.gov.uk/output/Page63.html

———, "Subversion," Web page, undated(e). As of January 10, 2009: http://www.mi5.gov.uk/output/subversion.html

———, *The Security Service: MI5*, London: Her Majesty's Stationery Office, 1993.

Security Service, and Central Office of Information, *The Security Service: MI5*, 3rd ed., London: Her Majesty's Stationery Office, 1998.

Security Service Act 1989 (c. 5). As of October 27, 2008: http://www.opsi.gov.uk/acts/acts1989/ukpga_19890005_en_1

Security Service Act 1996 (c. 35). As of October 27, 2008: http://www.opsi.gov.uk/acts/acts1996/ukpga_19960035_en_1

Senate Legal and Constitutional References Committee, *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002 and Related*

Matters, Canberra, December 2002. As of October 22, 2008: http://www.aph.gov.au/Senate/committee/legcon_ctte/completed_inquiries/2002-04/Asio_2/report/report.pdf

Shapiro, Jeremy, and Bénédicte Suzan, "The French Experience of Counter-Terrorism," *Survival*, Vol. 45, No. 1, Spring 2003, pp. 67–98. As of October 23, 2008: http://www.brookings.edu/views/articles/fellows/shapiro20030301.pdf

SIRC—*see* Security Intelligence Review Committee.

Smolar, Piotr, "*La Création d'un Service Unique pour le Renseignement Intérieur se Précise*," Le Monde, May 17, 2006.

Stanley, Trevor, "Australian Anti-Terror Raids: A Serious Plot Thwarted," *Terrorism Monitor*, Vol. 3, No. 23, December 2, 2005. As of October 28, 2008: http://www.jamestown.org/terrorism/news/article.php?issue_id=3546

Stewart, Sir Findlater, report, November 27, 1945, in Baron Alfred Denning, *The Denning Report: The Profumo Affair*, London: Pimlico, 1963, 1992 reprint.

Stewart, Ian, "Airport Attack Puts Britain on High Alert," *Arizona Republic*, July 1, 2007.

Stock, Jürgen, and Annette Herz, "The Threat Environment Created by International Terrorism from the German Police Perspective," *European Journal on Criminal Policy and Research*, Vol. 13, No. 1–2, April 2007, pp. 85–108.

Stone, David J. A., *Fighting for the Fatherland: The Story of the German Soldier from 1648 to the Present Day*, London: Conway, 2006.

Stora, Benjamin, *Algeria, 1830–2000: A Short History*, Ithaca, N.Y.: Cornell University Press, 2001.

Sünkler, Sören, *Die Spezialverbände der Bundeswehr*, Stuttgart: Motorbuch, 2006.

Sweeney, John, *At Scotland Yard: Being the Experiences During Twenty-Seven Years' Service of John Sweeney*, Francis Richards, ed., London: Grant Richards, 1904.

"Sydney Nuclear Power Plant Was a Possible Target," *Nation* (Bangkok), November 15, 2005.

"Terror Swoop: More Arrests Likely," CNN.com, November 9, 2005. As of February 8, 2006: http://edition.cnn.com/2005/WORLD/asiapcf/11/07/australia.terror

Terrorism: Special Investigation Techniques, Strasbourg: Council of Europe Publishing, April 2005.

Thuillier, François, *L'Europe du Secret: Mythes et Réalité du Renseignement Politique Interne*, Paris: La Documentation française, 2000.

Todd, Paul, and Jonathan Bloch, *Global Intelligence: The World's Secret Services Today*, London: Zed Books, 2003.

Tophoven, Rolf, *GSG 9: Kommando gegen Terrorismus*, Koblenz and Bonn: Wehr und Wissen, 1977.

Treverton, Gregory F., *Reorganizing U.S. Domestic Intelligence: Assessing the Options*, Santa Monica, Calif.: RAND Corporation, MG-767-DHS, 2008. As of October 21, 2008:
http://www.rand.org/pubs/monographs/MG767/

UCLAT—*see* Unité de Coordination de Lutte Anti-terroriste.

Uhlmann, Janette, "L'islamisme Radical et le Jihadisme en Allemagne," in Jean-Luc Marret, ed., *Les Fabriques du Jihad*, Paris: Presses Universitaires de France, 2005.

"UK Rejects Sarkozy's Mosque Surveillance Plan," Agence France-Presse, Brussels, July 13, 2005.

Unite de Coordination de Lutte Anti-terroriste, "The 'Vigipirate' Plan," January 2005.

UNSTR—*see* Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism.

U.S. Congress, 109th Congress, 2nd Session, *Making Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 30, 2007, and for Other Purposes: Conference Report (to Accompany H.R. 5441)*, September 28, 2006. As of October 10, 2008:
http://purl.access.gpo.gov/GPO/LPS75576

U.S. Department of Homeland Security Office of the Inspector General, *Survey of DHS Intelligence Collection and Dissemination (Unclassified Summary)*, Washington, D.C., OIG-07-49, June 5, 2007. As of October 13, 2008:
http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07-49_Jun07.pdf

U.S. General Accounting Office, *Combating Terrorism: How Five Foreign Countries Are Organized to Combat Terrorism: Report to Congressional Requesters*, Washington, D.C., GAO/NSIAD-00-85, April 2000. As of October 28, 2008:
http://www.gao.gov/products/NSIAD-00-85

Venice Commission—*see* European Commission for Democracy Through Law.

Vercher, Antonio, *Terrorism in Europe: An International Comparative Legal Analysis*, Oxford: Clarendon Press, 1992.

Villatoux, Paul, "*Affaire Georges Besse: Action Directe Déclare la Guerre à l'État Français*," Police Pro, Vol. 4, July 2007. As of October 23, 2008:
http://police-pro.histoireetcollections.com/article-21580-l-affaire-georges-besse-action-directe-declare-la-guerre-a-l-etat-francais.html

Violet, Bernard, *Carlos: Les Réseaux Secrets du Terrorisme International*, Paris: Seuil, 1996.

"War on Dissent," *Timeframe*, Web page, undated. As of June 15, 2007: http://www.abc.net.au/time/episodes/ep8a.htm

Weisburd, David, and Anthony Allan Braga, eds., *Police Innovation: Contrasting Perspectives*, Cambridge and New York: Cambridge University Press, 2006.

"Werthebach Views Threat from Extremism," *Focus*, June 15, 1993.

Whitehead, Phillip, *The Writing on the Wall: Britain in the Seventies*, London: M. Joseph, 1985.

Whitlock, Craig, "French Push Limits in Fight on Terrorism," *Washington Post*, November 2, 2004, p. A01. As of October 28, 2008: http://www.washingtonpost.com/wp-dyn/articles/A17082-2004Nov1.html

Windrow, Martin, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, London: Weidenfeld and Nicolson, 2004.

Wright, Lawrence, *The Looming Tower: Al-Qaeda's Road to 9/11*, London: Allen Lane, 2006.

Zamponi, Francis, "RG, DST, SDECE, DGSE: Un Demi-siècle de Dérives," in Roger Faligot, Jean Guisnel, and Rémi Kauffer, eds., *Histoire Secrète de la Ve République*, Paris: La Découverte, 2006.