



**CFIS:
A FOREIGN INTELLIGENCE SERVICE FOR CANADA**



Canadian Defence
& Foreign Affairs
Institute

CFIS:
A Foreign Intelligence Service for Canada

Barry Cooper

“An army without secret agents is
like a man without eyes and ears.”

– Sun Tzu, *The Art of War*

November 2007
Prepared for the Canadian Defence & Foreign Affairs Institute
1600, 530 – 8th Avenue SW, Calgary, AB T2P 3S8
<www.cdfai.org>
©Canadian Defence & Foreign Affairs Institute

**OTHER PUBLICATIONS WRITTEN FOR OR ASSISTED BY:
THE CANADIAN DEFENCE & FOREIGN AFFAIRS INSTITUTE**

- Canada as the “Emerging Energy Superpower”: Testing the Case**
Annette Hester October 2007
- A Threatened Future: Canada’s Future Strategic Environment and its Security Implications**
J.L. Granatstein, Gordon S. Smith, and Denis Stairs September 2007
- Report on Canada, National Security and Outer Space**
James Fergusson and Stephen James June 2007
- Conflict in Lebanon: On the Perpetual Threshold**
Tami Amanda Jacoby April 2007
- Canada in Afghanistan: Is it Working?**
Gordon Smith March 2007
- Effective Aid and Beyond: How Canada Can Help Poor Countries**
Danielle Goldfarb December 2006
- The Homeland Security Dilemma: The Imaginations of Failure and the Escalating Costs of Perfecting Security**
Frank Harvey June 2006
- An Opaque Window: An Overview of Some Commitments Made by the Government of Canada Regarding the Department of National Defence and the Canadian Forces; 1 January 2000 – 31 December 2004**
David J. Bercuson, Aaron P. Plamondon, and Ray Szeto May 2006
- The Strategic Capability Investment Plan: Origins, Evolution and Future Prospects**
Elinor Sloan March 2006
- Confusing the Innocent with Numbers and Categories: The International Policy Statement and the Concentration of Development Assistance**
Denis Stairs December 2005
- In the Canadian Interest? Assessing Canada’s International Policy Statement**
David J. Bercuson, Derek Burney, James Fergusson, Michel Fortmann/Frédéric Mérand, J. L. Granatstein, George Haynal, Sharon Hobson, Rob Huebert, Eric Lerhe, George Macdonald, Reid Morden, Kim Richard Nossal, Jean-Sébastien Rioux, Gordon Smith, and Denis Stairs October 2005
- The Special Commission on the Restructuring of the Reserves, 1995: Ten Years Later**
J. L. Granatstein and LGen (ret’d) Charles Belzile September 2005
- Effective Defence Policy for Responding to Failed and Failing States**
David Carment June 2005
- Two Solitudes: Quebecers’ Attitudes Regarding Canadian Security and Defence Policy**
Jean-Sébastien Rioux February 2005
- In The National Interest: Canadian Foreign Policy in an Insecure World**
David J. Bercuson, Denis Stairs, Mark Entwistle, J. L. Granatstein, Kim Richard Nossal, and Gordon S. Smith October 2003
- Conference Publication: Canadian Defence and the Canada-US Strategic Partnership September 2002
- To Secure A Nation: The Case for a New Defence White Paper**
David J. Bercuson, Jim Fergusson, Frank Harvey, and Rob Huebert November 2001

TABLE OF CONTENTS

Executive Summary	i
Sommaire en Français	ii
Acknowledgements	iii
Definitions and Abbreviations	iv
1. Introduction: Why Spy?	1
2. History of Canadian Foreign Intelligence	10
2 (a) Origins	10
2 (b) The Great War	10
2 (c) Inter-war Years	11
2 (d) World War II	12
2 (e) No Foreign Intelligence Service for Post-war Canada	14
2 (f) Post-war Counter-intelligence	18
2 (g) The Birth of the CSIS	21
2 (h) Collection of Information Concerning Foreign States and Persons	23
3. The Canadian Foreign Intelligence Community Today	25
3 (a) Communications Security Establishment	25
3 (b) Canadian Security Intelligence Service	26
3 (c) Department of National Defence	31
3 (c) i Yugoslavia	34
3 (c) ii Somalia	34
3 (c) iii Rwanda	35
3 (c) iv Zaïre	36
3 (d) Other Government Units	37
4. Problems	39
4 (a) No Interest in Foreign Intelligence	39
4 (b) Intelligence Dependence	40
4 (c) The Downside of Intelligence Sharing	43
4 (d) SIGINT – Putting All of Canada’s Intelligence Eggs in One Basket?	44
4 (e) Threats to Canada	47
4 (e) i Terrorism	47
4 (e) ii Economic Espionage	47
4 (e) iii State-sponsored Espionage	48
5. Why Canada Needs a Foreign Intelligence Agency	49
5 (a) Canadian Intelligence Needs	49
5 (a) i Political Intelligence	49
5 (a) ii Economic Intelligence	51
5 (a) iii Defence Intelligence	51
5 (a) iv Alliance Contributions	52
5 (b) Foreign Intelligence: Arguments Against	53
5 (b) i Cost Prohibitive	53
5 (b) ii Inexperience	54
5 (b) iii Reputation	54

TABLE OF CONTENTS (CONT.)

5 (c)	Foreign Intelligence: Arguments For	55
5 (c) i	Problems with Intelligence Sharing	55
5 (c) ii	Information Sovereignty	55
5 (c) iii	National Protection	56
5 (d)	A Problem Restated	57
6.	CFIS	60
6 (a)	CSIS – Spycatchers and Spies	60
6 (a) i	Why Spycatchers and Spies Should Remain Separate	60
6 (b)	A Canadian Foreign Intelligence Service – Where and Why?	63
6 (b) i	Importance of Analysis	65
6 (b) ii	Focal Point for Canadian Intelligence	66
6 (b) iii	Accountability	67
6 (b) iv	Reforming Military Intelligence	68
7.	Conclusion	69
	Bibliography	71

EXECUTIVE SUMMARY

The Canadian security and intelligence community is focused on domestic threats. These are important, no doubt, but in an increasingly globalized world, where neither travel, commerce, communication, and especially conflict, are domestic, it has become necessary to develop a capacity for acquiring timely intelligence regarding the intentions and capabilities of foreign states, corporations, and non-state political and religious actors. After the terrorist attack of 11 September 2001, it became self-evident that the end of the Cold War did not bring an end to hostility to Western and other market-based democracies. Canada's post-Cold War enemies are hidden, and Canada's diplomatic and military allies have remained economic competitors. On those grounds alone, Canada needs a Foreign Intelligence Service, CFIS, with a mandate similar to that given CSIS in the area of domestic or security intelligence. Canada did not establish a foreign intelligence agency after World War II, apparently because of the bureaucratic sensibilities of senior officials in the Department of External Affairs. One of the long-term consequences of the willful ignorance of intelligence matters has been felt in the conduct of Canadian foreign policy, particularly in recent years as the strenuous experiences of the Cold War fade from memory and the men and women who lived through that half century of conflict retire. It is a basic reality concerning the conduct of foreign policy, however, that if it is not shaped by intelligence, it is bound to be shaped by ignorance.

This deliberate neglect was not a total neglect, but it has meant that Canada is a net consumer of intelligence produced by others for their own purposes. Canada has been a member of several intelligence-sharing alliances and has made a virtue of necessity by claiming that the country receives all the intelligence it needs from its allies. In fact, without an independent source of foreign intelligence, there is simply no way at all to verify this claim. By refusing to use secret foreign intelligence gathering, Canada fails to do all it can to provide industry with the information needed to compete successfully in foreign markets, to say nothing of wider political matters.

In its most recent public report, CSIS noted that intelligence collection is based on information obtained from "members of the public, foreign governments and technical interception of telecommunications ... combined with information from open sources including newspapers, periodicals, academic journals, foreign and domestic broadcasts, official documents and other published material." In short, Canada relies on everything but spying. This paper argues the case for creating a foreign intelligence service – spies. Recent press reports indicate that, apparently on the advice of CSIS, the Harper government is considering expanding the remit of CSIS to include foreign intelligence. This is a bad idea for two reasons. First, as the example of the KGB indicates, it is never a good idea to house spies and counter-spies under the same administrative roof. Second, one should never forget that the first task of an organization, including one engaged in security intelligence such as CSIS, is to preserve itself and to grow. Security and foreign intelligence are quite different. In fact, the CSIS initiative confirms the argument of this paper: Canada needs spies.

SOMMAIRE EN FRANÇAIS

Les milieux canadiens de la sécurité et des renseignements concentrent leur attention sur les menaces émanant de l'intérieur. Il ne fait aucun doute que celles-ci sont importantes, mais, dans un monde de plus en plus globalisé, où ni les voyages, ni le commerce, ni les communications, ni, particulièrement, les conflits sont confinés au niveau intérieur, il est devenu nécessaire de développer une capacité d'acquérir des renseignements d'actualité concernant les intentions et les capacités d'États, de sociétés et d'acteurs politiques et religieux non étatiques étrangers. Après l'attaque terroriste du 11 septembre 2001, il nous est apparu qu'il allait de soi que la fin de la Guerre froide n'avait pas fait cesser l'hostilité entre l'Ouest et d'autres démocraties fondées sur le marché. Les ennemis du Canada, dans l'après-guerre froide, sont cachés, et les alliés diplomatiques et militaires du Canada sont demeurés des concurrents économiques. Sur ces motifs seuls, le Canada a besoin d'un service du renseignement extérieur qui soit doté d'un mandat semblable à celui qu'on donne au SCRS dans les domaines du renseignement intérieur ou du renseignement de sécurité. Le Canada n'a pas établi d'organisme de renseignement étranger. après la Deuxième Guerre mondiale, apparemment à cause des sensibilités bureaucratiques de hauts dirigeants du ministère des Affaires étrangères. Une des conséquences à long terme de l'ignorance consentie des questions de renseignement s'est fait sentir dans la conduite de la politique étrangère du Canada, particulièrement ces dernières années, à mesure que s'atténue la mémoire des expériences pénibles de la Guerre froide, particulièrement ces dernières années, où des hommes et des femmes qui ont vécu à travers ce demi-siècle de conflits sont en train de prendre leur retraite. C'est toutefois une réalité de base en matière de conduite des affaires étrangères, que si celle-ci n'est pas informée par les renseignements, elle ne peut faire autrement que l'être par l'ignorance.

Cette négligence délibérée n'a pas été une négligence totale, mais elle a signifié que le Canada est un consommateur net de renseignements produits par d'autres pour leurs propres objectifs. Le Canada est membre de plusieurs alliances de partage des renseignements et a fait de la nécessité une vertu en prétendant que le pays reçoit de ses alliés tous les renseignements dont il a besoin. En fait, sans une source indépendante de renseignements touchant l'étranger, il n'y a tout simplement aucune façon possible de vérifier cette affirmation. En refusant d'utiliser une collecte secrète de renseignements touchant l'étranger, le Canada est incapable de faire tout ce qu'il peut pour donner à l'industrie les renseignements dont elle a besoin pour livrer une concurrence avec succès sur les marchés étrangers, pour ne pas mentionner les questions politiques plus étendues.

Dans son rapport public le plus récent, le SCRS note que la collecte de renseignements est basée sur l'information obtenue de « membres du public, de gouvernements étrangers et de l'interception technique des télécommunications combinée aux renseignements provenant de sources ouvertes, dont les journaux, les périodiques, les journaux académiques, les émissions étrangères et intérieures, les documents officiels et autre documentation publiée. » En bref, le Canada se fie à tout sauf à l'espionnage. La présente étude débat du cas de la création d'un service du renseignement extérieur, c'est-à-dire d'espions. Des rapports publiés récemment dans la presse indiquent que, apparemment sur l'avis du SCRS, le gouvernement Harper songe à agrandir l'aire d'action du SCRS pour inclure le renseignement extérieur. Il s'agit là d'une mauvaise idée pour deux raisons. La première, comme l'indique l'exemple du KGB, ce n'est jamais bien de loger l'espionnage et le contre-espionnage sous le même toit administratif. La deuxième, c'est qu'on ne devrait jamais oublier que la première tâche d'une organisation, y compris une organisation engagée dans le renseignement extérieur comme le SCRS, c'est de se préserver elle-même et de croître. Les renseignements de sécurité et les renseignements extérieurs sont tout à fait différents. En fait, l'initiative du SCRS confirme l'argument de cette étude: le Canada a besoin d'espions.

ACKNOWLEDGEMENTS

This study began when I was associated with the Fraser Institute, the members of which often had some difficulty comprehending the need to study military and security policy. The CDFAI, in contrast, has a mandate to study and analyze these matters, which expresses a kind of rationality in the division of labour among Canadian research institutes. Both institutes supported my application of the insights of Western political philosophy, my main academic concern, to questions and problems conventionally discussed only by economists, historians, or specialists in international relations. Only a churl would be ungrateful, so I must thank them both.

I must also thank several students at the Centre for Military and Strategic Studies at the University of Calgary and a number of colleagues at that centre of excellence as well. They have served as research associates and sounding boards, not least of all in my graduate course on war and interpretation. Because of the current employment status of some, I will not name them. Thank you anyway. You know who you are, and you know who to blame for any remaining errors. I must also thank the anonymous pre-publication readers of this report for their useful criticism.

Finally, I must thank the Donner Canadian Foundation and Joe Donner Jr. for their support and encouragement.

Thanks are also owed to Mirja van Herk for her endless word processing, to JoAnn Cleaver for her edits, and to James B.C. Doak for his support.

DEFINITIONS AND ABBREVIATIONS

These definitions are taken from NATO (2006) or from Department of National Defence documents (Canada, 2000h; 2003d; 1996a).

Anti-terrorism – All defensive and preventive measures taken to reduce the vulnerability of forces, individuals, and property to terrorism. Note: such measures include protective and deterrent measures aimed at preventing an attack or reducing its effect(s).

Clandestine operation – Operation related to intelligence, counter-intelligence, and other similar activities, sponsored or conducted in such a way as to assure secrecy or concealment.

Counter-intelligence – Those activities concerned with identifying and counteracting the threat to security posed by hostile intelligence services or organizations or by individuals engaged in espionage, sabotage, subversion, or terrorism.

Counter-terrorism – All offensive measures taken to neutralize terrorism before and after hostile acts are carried out. Note: such measures include those counterforce activities justified for the defence of individuals as well as containment measures implemented by military forces or civilian organizations.

Foreign intelligence – Intelligence concerning the plans, capabilities, activities, or intentions of foreign states, organizations, or individuals. It is collected to help promote, as well as to safeguard, national interests. Moreover, foreign intelligence need not have a threat component.

HUMINT – Intelligence collected by human beings, whether secret or not, whether stolen or free, and from open sources.

Information – Unprocessed data of every description which may be used in the production of intelligence.

Intelligence – The product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity.

Open source intelligence – Intelligence derived from publicly available information and other unclassified information that has limited public distribution or access.

Security intelligence – Intelligence regarding the identity, capabilities, and intentions of hostile organizations or individuals who are, or who may be, engaged in espionage, sabotage, subversion, terrorism, criminal activity, or extremism. It is collected to help maintain public safety and to protect national security.

SIGINT – Signals intelligence – intelligence gathered electronically from a variety of electromagnetic signals.

Strategic intelligence – Intelligence required for the formulation of policy, military planning, and the provision of indications and warnings, whether at national and/or international levels.

1. INTRODUCTION: WHY SPY?

Canada lacks a government agency similar to the American CIA or the British MI6 that is specifically tasked to collect or steal foreign human intelligence (HUMINT). Throughout this paper, I refer to what such a notional agency would be named as the Canadian Foreign Intelligence Service (CFIS). Had Canada followed the Australian Secret Intelligence Service (ASIS) or the British Secret Intelligence Service (BSIS or MI6), the Canadian version would be called the Canadian Secret Intelligence Service, CSIS. But we already have a CSIS, the Canadian Security Intelligence Service. However, security (defensive) and foreign (offensive) intelligence are different and thereby require different kinds of agencies. At the very least, Canadians and their elected representatives need to become aware of the arguments in favour of the CFIS. If nothing else, this paper will perhaps help initiate, or even contribute to, a discussion of a question that is too important to simply be left to bureaucrats in CSIS.

During the Cold War, Canada relied heavily on its allies, particularly the United States, to provide foreign intelligence. Since the end of World War II, Canada has been a net consumer of intelligence, particularly human intelligence, rather than a net producer. It has, moreover, grown accustomed to living with an “intelligence deficit.” This was already a serious problem during the Cold War; the terrorist attacks of 11 September 2001 exposed a new and dangerous consequence of a longstanding Canadian tradition of relying on allies and punching below its weight. In an era of asymmetric unconventional warfare, high technology tools of signals intelligence collection, for which Canada has an acknowledged competence, are of reduced importance. Clandestine human intelligence is the most valuable commodity, yet it is in the shortest supply. There is no well defined battlefield on which to fight and consequently no conventional front lines behind which to gather intelligence. The first thing to note, therefore, is that this examination of the need for Canada to develop a foreign intelligence capability is taking place in an unprecedented context of asymmetric warfare and covert terrorist operations. Second, as Ted Parkinson observed recently, “no *serious* in-depth study available in the public domain examining *all* the issues has ever been conducted” (Parkinson 2006). There have been, however, several studies over the years that have advocated for, or detracted from, the establishment of a CFIS.¹ This study may not have examined all the issues, but it aims to examine the major elements involved in the establishment of a foreign intelligence service, and in that respect, at least, aspires to be serious.

An index of the gravity of the issue is suggested by the observation that even the formidable American intelligence community was unable to collect accurate and timely intelligence regarding al-Qa’ida prior to the attacks of 11 September 2001. As the final report of the 9/11 Commission stated:

The September 11 attacks fell into the void between foreign and domestic threats. The foreign intelligence agencies were watching overseas, alert to foreign threats to US interests there. The domestic agencies were waiting for evidence of a domestic threat from sleeper cells within the United States. No one was looking for a foreign threat to domestic targets. The threat that was coming was not from sleeper cells. It was foreign – but from foreigners who had infiltrated into the United States. (United States 2004, 263)

¹ See Starnes 1982, 1987, 1992; Whitaker 1991; Finn 1993; Hensler 1995; Sallot 1996; Wark 2001; Weller 2001; Brown 2001; Chwialkowska 2001; Pratt 2003; Stairs 2003; Travers 2004; McClintock 2004; Gordon 2004; Bell 2005; Morden 2006; and Mayeda 2007.

The failure of American intelligence was not some kind of generic shortcoming, the commission said, but a specific and four-fold failure in imagination, policy, capabilities, and management (United States 2004, 339). One important implication for Canada is that even the United States may, under some circumstances, have little to share. This leaves Canada vulnerable and blind, for the simple and obvious reason that, without national intelligence assets operating abroad, it must wait for its allies to share any foreign intelligence that they, in fact, may not have or may not wish to share. As is outlined in detail below, because Canada is a net importer of intelligence, the exporters can, and no doubt do, influence Canadian foreign policy agenda by exporting what serves the exporter's interests (Canada 2003a).

Moreover, where Canada does produce intelligence from foreign sources – chiefly military intelligence – after-action analysis of peacekeeping missions in Rwanda, Somalia, and Yugoslavia exposed grave shortcomings in existing Canadian intelligence capabilities. In the context of an evolving terrorist threat, foreign intelligence will be essential to identify potential hostiles before they reach Canada. Likewise, the possibility that Canada will be marginalized in a combined, binational North American Defence Command (should it be created) as well as within existing global intelligence alliances underlines the need for independently collected, foreign HUMINT. Given the limitations of the Canadian intelligence community, the question, Should Canada create its own secret intelligence service? seemingly answers itself. Churchill once observed that every country has an army; either its own or someone else's. The same is true of spies and for the same reasons: they are needed to preserve independence.

In the past several years, there have been a number of what might be called public musings by members of the Canadian intelligence community about the need to establish such an agency. As long ago as 1982, for example, John Starnes established something like the baseline orthodoxy. There is, he said, “no glaring example in the past 25 years where our interests have suffered simply because we ourselves have been unable to covertly collect intelligence in other countries” (9). Now, John Starnes was a long-serving member of the RCMP security service, eventually its first civilian director, and before that, a senior official in the Department of External Affairs (Starnes 1998). Notwithstanding his vast experience, a little reflection indicates that his remarks are completely counterfactual, a classic instance of an unknown unknown – an “unk-unk” as the engineers at NASA (and former United States Secretary of Defense Donald Rumsfeld) call such hidden silences. How can anyone, including Starnes, possibly know what Canadian foreign intelligence might have found out without the ability to find out?

Twenty years later, the official position of the Government of Canada had not changed. On 5 October 2001, Foreign Affairs Minister John Manley wondered aloud at a news conference about the need to establish a foreign intelligence agency (Brown 2001); a few months later, his musings took the opposite tack: “I don't see it [the creation of a CFIS] as an immediate priority. I think it is one of those deeper issues that requires a lot more careful thought and consideration. In the meantime, I think the resources we're giving CSIS enable it to do more collection of information outside Canada” (Ljunggren 2002, A1). Even more recently, in April 2007, CSIS Director Jim Judd told the Senate Committee on National Security and Defence (SCONSAD) that Canada cannot fully meet its intelligence requirements without a CFIS, which seemed to indicate that he supported the position of the Harper government as it was articulated during the 2006 election campaign (Mayeda 2007b, 2007c). At that time, the Conservative Party promised, if elected, to create a foreign intelligence capability. A couple of weeks after Judd spoke to the Senate committee, Public Safety Minister Stockwell Day told the Commons Public Safety Committee that the government no longer favoured establishing a CFIS, but that it would prefer to expand the remit of CSIS (Mayeda 2007d). Two weeks later, Judd agreed in public with his political boss (Galloway 2007). Such indecisiveness articulated within such a short period of time indicates that

both the government and the security and intelligence community in Canada remain unsure of the proper way to proceed. They do, however, appear to be aware of the problem.

With respect to the latest position, as noted below, giving CSIS resources to operate outside Canada is a highly questionable policy on both legal and operational grounds. The first problem can be rectified by changing the terms of the CSIS Act. The second remains a poor policy choice even though it increases the bureaucratic clout of CSIS.

Indecision has plagued the history of security and intelligence issues in Canada. Prior to the recent flurry of activity in May 2002, the House of Commons Standing Committee on National Defence and Veterans Affairs (SCNDVA) recommended that the government review Canada's security and intelligence structure with a view to determining whether an independent CFIS was needed. The response was as predictable as it was dismissive: security and intelligence has been enhanced since 9/11; foreign intelligence is already available from the Communications Security Establishment (CSE), from the Department of Foreign Affairs (DFAIT), and from Canada's allies; and finally:

The issue of a foreign intelligence service arises from time to time. It is healthy to examine this idea and to assess the adequacy of our intelligence capabilities and products ... At present, the Government believes that the establishment of a separate Canadian foreign intelligence agency would be premature. (Canada 2002k)

As outlined below, CSE deals only with signals intelligence, whereas DFAIT gathers chiefly open-source information and has no dedicated espionage capability. One of this study's principal contentions is that there are inherent and obvious limits to intelligence sharing with allies. None of these factors deals at all with the purpose and capability of a foreign intelligence service.

The first ever statement on Canadian national security was issued in April 2004. Prior to the publication of *Securing an Open Society* (Canada 2004a), Canada lacked a national security framework, that is, a clear statement of what constitutes Canadian national security in the context of the global security environment that has a direct focus on Canadian national interests. It was the first time Canada produced a document comparable to the American statement on *National Security Strategy* or the British *Strategic Trends*. Unfortunately, the authors did not take the opportunity to reconsider the traditional view with respect to a CFIS. Instead the report reiterated the received position: "No changes to the current mandates and structures of Canada's security and intelligence agencies are being proposed at this time ... Given the security threats facing Canada and our allies, we will devote a greater proportion of our efforts to security intelligence" (Canada 2004a). Whatever foreign intelligence Canada obtains, the report continued, would come from "working with our allies." The reason offered is that Canada simply cannot do foreign intelligence: "Canada alone could not replicate the benefits gained through these international arrangements. But we are also a significant contributor of intelligence. These contributions are recognized and appreciated by our allies" (Canada 2004a). This statement is disingenuous at best. No one has ever suggested that Canada try to replicate the business of MI6 or CIA, only that Canada contribute its share to a common intelligence pool. Moreover, the notion that Canada's allies consider the country a significant contributor of intelligence seriously overstates the appreciation and recognition accorded by Canada's allies.

There was some acknowledgement of the problem of an absent foreign intelligence capability in a report issued later in 2004 by the Department of Public Safety and Emergency Preparedness (PSEPC). In a brief discussion of the "Canadian Intelligence Resource Centre," there is the following account:

Canadian Foreign Intelligence Service [non-existent]

Canada still thinks today that the financial cost, the political risk, and the absence of clear and present threats to Canadian national security militate against the creation of a foreign intelligence service. (Canada 2004b)

By “political risk,” the government typically means risk to the image of Canada held by senior officials in the Department of Foreign Affairs. The real, not imaginary, political risk is that, by contributing so little, Canada may be excluded from sharing in intelligence gained by others. It may be reassuring to the author of this report on public safety that there is an “absence of clear and present threats to Canadian national security.” It is, however, a maxim of sound intelligence gathering that, in the words of former Director of Central Intelligence William Casey, “the absence of evidence is not evidence of absence” (quoted in Davis 2003). Indeed, one can quite reasonably speculate that Canadian officials are willing to justify the absence of a CFIS on the grounds that they do not know enough to know that Canada needs such an organization.

Anne McLellan, deputy prime minister and minister of PSEPC (as she then was), also pronounced on this question (Canada 2005a). In testimony before the Standing Senate Committee on National Security and Defence (SCONSAD), Senator Michael Forrester asked her about her support for a broader-based CSIS collection capability offshore, both quiet intelligence – not threat-related – and otherwise.

Have you been able to divert some additional funds to CSIS for this activity? Is it showing up in a higher quality of work and improved work?

Ms. McLellan: I have made a budgetary request for this year ... that would permit the gathering of additional foreign intelligence, and it is one of the things that I have talked about before and the fact that we live in a world where it is incumbent upon each of us as countries and allies to ensure that we are doing our fair share, both in terms of being able to protect our own people and having that which we share under appropriate circumstances around foreign security intelligence with our allies.

While CSIS does collect foreign security intelligence now, I have made no secret of the fact that they it [sic] collect more. I have made a budgetary request to that effect.

The Chairman: I take it from that, minister, that CSIS will be collecting non-threat related intelligence?

Ms. McLellan: No.

The Chairman: I take from that that government has made a decision that foreign intelligence is properly the purview of CSIS and not some other agency?

Ms. McLellan: No final determination has been made in that regard. I am making a request for funding to permit us to collect more foreign security intelligence. I have not indicated where the locus of that gathering would be. (Canada 2005a)

The questions from the chairman, Senator Kenny, that CSIS might collect non-threat-related foreign intelligence was as significant as the response of the minister. The distinction, dealt with below in some detail, between foreign intelligence which may or may not be threat-related, and

security intelligence, which is necessarily threat-related, is fundamental. Ms. McLellan said: (1) that CSIS would not have its mandate expanded to cover foreign intelligence gathering (spying), and (2) that no decision had yet been made about expanding the CSIS mandate or creating a foreign intelligence service, CFIS.

Equally significant, McLellan noted that allied interdependence is also important in two respects: (1) “doing our fair share,” and (2) sharing “around foreign security intelligence with our allies.” Most who have examined Canadian intelligence production to allies, as distinct from consumption from allied intelligence sources, have concluded that Canada is far from doing its fair share, however that may be measured. The second point McLellan made, as befits one in charge of intelligence, was essentially made in code. The term “foreign security intelligence” is a hybrid and ambiguous term (discussed below) that refers to intelligence gathered abroad that has a bearing on the domestic security of Canada. It is not spying. It is “defensive” intelligence, not offensive, more akin to an FBI operation outside the United States than to a CIA one. The problem she was alluding to was this: Canada can collect security intelligence abroad by way of CSIS, and since by definition security intelligence deals with threats to Canada and not to allies, CSIS is prohibited by law from taking action should its investigations in foreign parts uncover a threat to an ally. That would be spying and CSIS does not spy. As Martin Rudner told this same senate committee a couple of years earlier, the limitation on what CSIS could do “could create a gap that could have horrendous consequences” (Canada 2003a). One conclusion at least is clear: the federal government, whether liberal or conservative, is fully aware of the problems posed by an absence of a foreign intelligence capability for the country. It also knows that either CSIS legislation will have to be changed and more resources made available to it so that Canada can actually do its “fair share,” or a new agency dedicated to acquiring foreign intelligence will have to be created. As noted above and argued in detail below, the second alternative is preferable.

Most of the argument in favour of the second alternative, namely the creation of a CFIS, has been undertaken outside the government, either in parliamentary committees or by non-government experts. Until very recently, the same was true of analyses of the force structure of the Canadian military (see Cooper, Stephenson and Szeto 2004). The present report will review the evidence and the arguments in support of a Canadian Foreign Intelligence Service that would complement the existing Canadian Security and Intelligence Service. First, however, a number of assumptions and definitions, some of which have already been unobtrusively introduced, will be made explicit. These remarks are followed by a brief history of Canadian intelligence capabilities, a description of the current Canadian intelligence community and its problems, and finally, with how the addition of a foreign intelligence agency might address those problems.

The most basic assumption made is that conflict is inevitable, that knowledge of friends and of enemies matters in conflict, and that it can occasionally prove decisive. The Duke of Marlborough was of the opinion that “no war can be conducted successfully without early and good intelligence.” For George Washington, it was self-evident that “the necessity of procuring good intelligence is apparent and need not be further argued” (quoted in Keegan 2003, 5). Intelligence is, therefore, an instrument of conflict. Unlike a weapon, however, it may not wound, but it most certainly has killed millions and preserved other millions.

Intelligence is always ancillary. At the outset of a conflict, no one seeks to prevail by attrition, which is why it is important to reduce the cost of victory by thought and intelligence. However, at the end of the day, force, not fraud (to use Machiavelli’s terminology), is what counts. And yet, however sharp one’s sword, one must know where to place it. In the conduct of foreign policy and security policy, such knowledge is called “intelligence.” It is, therefore, more than information. Indeed, “information does not become intelligence until somebody recognizes its importance,” and its importance is conditioned by strategy, and thus by policy – especially foreign policy (Codevilla

1992, 387). If Canada decides to recreate a foreign intelligence capability, that will result from a serious and strategic policy decision; if Canada continues to conduct its foreign and defence policy without such a capability, that will also be a policy decision.

As the government's response to the 2002 SCNDVA report said, it is healthy to examine the role of intelligence agencies from time to time. What the government did not add, however, is that such an examination seeks to determine how they fit into a coherent and reasoned list of requirements – a strategy. As Codevilla put it, “in espionage there is good long-term planning and bad long-term planning. But there can be no good short-term planning” (1992, 309). Codevilla had the United States in mind, but his insight applies equally to Canada or to any other country. Moreover, in the post-Cold War context where threats are more diffuse and less intense, more (not less) coherence, rationality, and insight is needed. For Canada, constrained both by its size and by its economic and geo-strategic circumstances (that is, by the fact that Canada has but one ally that counts), a great deal of realism is needed: the menu of options is limited.

Intelligence organizations co-operate across boundaries on a regular basis, but it is not done out of sheer good will and friendliness. It is done for the usual self-interested motives of important politicians and bureaucrats as well as for reasons of state and national interests. Intelligence operations always involve fine distinctions: there are those, for example, who say there are no friendly intelligence services but only intelligence services of friendly governments. As Granatstein and Stafford put it, “states have no friends, only interests, and this means that even allies are considered legitimate targets of espionage” (1990, 17). To be more precise, “friend-on-friend” spying may not be unheard of, but it is extremely rare for the very good reason that you need to trust your allies – an alliance is, by definition, a collective security arrangement. At one time, France sent agents to Canada to support Quebec separatists, which is one reason why even the mild-mannered Prime Minister Pearson reacted strongly to President DeGaulle's famous “Vive le Québec Libre!” speech (Black 1996, 50–51; Rudner 2001).

On the other hand, even the largest intelligence community in the world, that of the United States, not only makes major mistakes, it also has its own operational limitations. The Americans, for example, depend extensively on their colleagues in the French Directorate-General of External Security for a great deal of confidential information gathering in Africa. Moreover, relations among co-operating intelligence organizations are regulated by dozens, perhaps hundreds, of treaties and agreements establishing degrees of reciprocity, rights, permissions, and most important of all, the place of any particular intelligence agency in the great hierarchy of intelligence organizations worldwide. Most of these agreements are wholly or partially secret.

As noted above, the end of the Cold War disrupted many long-established intelligence alliances and routines. On the one hand, the disappearance of a stable, bipolar world meant there was less pressure on both sides to maintain the ability to conduct military espionage. On the other, globalization and technological change provided additional reasons, at least for industrialized states, to conduct high-tech spying. At the margin, this kind of intelligence-gathering is little more than commercial espionage. In addition, however, there are continuing issues of nuclear proliferation to consider (think of Iran or Pakistan), and as noted above, there is the on-going conflict with terrorists, chiefly al-Qa'ida, its affiliates, and states that have enabled al-Qa'ida to conduct its activities. In short, both Canada and the United States have adversaries. Accordingly, the need for intelligence is still present. Indeed, the end of the Cold War and of the routines built up over decades of confrontation have arguably made intelligence more important today than at any time since the end of World War II.

It is unlikely that the conflict with al-Qa'ida and its affiliates will end any time soon. Terrorist networks operate clandestinely, as do intelligence organizations. Their warfare is hidden and their

preparations are often silent as well. One of the implications of twenty-first century, asymmetric warfare, therefore, may be that it will entail a kind of role reversal (or at least an adjustment): instead of being simply an ancillary arm of military and foreign policy, intelligence organizations are increasingly on the (figurative) front lines.

The conventional description of intelligence proceeds in terms of four parts or constituents:

1. **Collection:** getting the facts, which may be simple or complex, static or changing, which also means that an intelligence agency needs to know what facts to collect. For example, religious affiliations and disputes, which for half a century have been ignored, count a great deal post-9/11.
2. **Analysis and Production:** screening important from trivial facts requires a serious and educated mind endowed with imagination. It is not, therefore, a conventional bureaucratic task, nor a job for committees.
3. **Counter-intelligence:** engaging hostiles in order to control what they know and do, unlike security, which typically protects against contact with hostiles. Counter-intelligence (CI) is inherently deceptive and also entails watching your own activities.
4. **Covert Action:** interfering in other countries' internal affairs, which is, after all, the whole point of foreign policy, including spying, which means stealing other peoples' secrets. After all, if they were not secret, you would not have to steal.

Taken together, it is clear that this understanding of intelligence reinforces the view that international relations involve intrigue. Accordingly, it is better to do it well because the option of not engaging in intrigue does not exist. By refusing to acknowledge the reality of deception and intrigue, you simply do it poorly. Self-blinding leads to ignorance, not to insight, nor does it lead to moral superiority (which is mostly self-deception anyhow), but to weakness.

The process of intelligence gathering has a bearing on the extent to which Canada needs a foreign intelligence capability. Because intelligence is information important for a specific policy question (conventionally termed raw intelligence), it matters a great deal whether a country that gathers intelligence shares it raw or shares the analysis of it – shares it cooked, so to speak. Analyzed intelligence has been cooked according to a specific recipe, or to abandon the metaphor, it has been produced for a specific policy purpose that animated the original collection. When analyzed intelligence is shared with an ally, it already bears the strong imprint of the interest of the collecting country. These interests need not be hostile. Indeed, shared intelligence from hostiles is usually disinformation. Even among close allies, however, analyzed intelligence reflects the interests of the producer, not the recipient.

Whether a country receives intelligence raw or cooked is important because raw intelligence can be analyzed to reflect the priorities and interests of the recipient. In addition, receiving raw intelligence is a good measure of the position of the recipient organization in the larger intelligence hierarchy. Peer or near-peer organizations typically share intelligence of equal value, whether raw or analyzed. From the early 1950s, as is discussed in more detail below, Canada and Australia formalized the kinds and extent of intelligence they would share; Canadian/American intelligence sharing has an even longer history.

At the same time, however, the senior partner can use intelligence sharing as a means of persuading allies to toe a line drawn by it. This is particularly true when the junior partner does not contribute much raw intelligence to their mutual exchanges. It is in the interests of Canada, therefore, to have something equivalent (though perhaps not equal) to share with the Americans,

not least of all because the United States remains the central hub in all intelligence alliances worldwide. To do so effectively means having a clear understanding of the strengths and weaknesses of the American intelligence community.

Necessarily, the mixture of strengths and weaknesses will provide both constraints and opportunities for Canada and for other close allies. For example, American intelligence has for many years been particularly strong in the area of technical intelligence gathering, especially signals intelligence and imagery (or SIGINT, as it is conventionally called). One consequence, as George Friedman said, is that “the tendency of the [American] intelligence community was to solve analytic problems with technical solutions” (2004, 72). In this example, the need for imaginative analysis provides an opportunity for a Canadian intelligence agency precisely because its personnel are external to the American intelligence community. The end of the Cold War and the reliance on the Department of Defence to carry out American foreign policy has increased rather than diminished dependence on high-tech intelligence (Priest 2003). Given the post-Cold War decline in the importance of human intelligence (Codevilla 1994, 240), the necessity for imaginative analysis is even greater.

The evolution of American intelligence gathering makes at least one thing clear: even Canada can develop a comparative advantage with respect to the United States. Moreover, as with comparative advantages in commerce, there are also benefits to be obtained on both sides from specialized intelligence gathering. In the broad context of the war against al-Qa’ida and its affiliates, a wider distribution of specialized skills and a mutual dependency among allies also ensures a greater defensive depth: if no one organization has a monopoly on skills, all organizations have an incentive to co-operate (Aldrich 2002).

As early as 2002, for example, Canadian military skills in the form of a highly trained light infantry formation with considerable experience in both conventional and unconventional operations – operations other than war, or OOTWar activities – were very useful to allied efforts in Afghanistan. Likewise the British Special Intelligence Service contributed a significant number of long-service intelligence people with local experience and language skills to the American-led operations in that country. In practice, American, British, Canadian, and Australian specialization proved complementary. Canadians benefited from having the ability to make a significant contribution – a contribution that made a difference. In this instance, the difference was military. In the future, Canada may be able to make a difference in terms of intelligence – provided the government makes the right long-term decisions now.

The issue of creating – or recreating – a foreign intelligence capability has been raised many times since the end of World War II. As we saw with recent responses, the government has generally been opposed to an expanded Canadian intelligence capability. Critics of a Canadian secret service make cogent arguments against such an agency, the foremost being cost (Globe and Mail 2007, A12). Given the government austerity of recent years, particularly in the areas of military and security policy, critics are justified in asking how such an organization would be funded. Again, critics note that if American intelligence, with its multi-billion dollar budget and global coverage developed over four decades during the Cold War, failed to predict the attacks on Washington and New York on September 11, how could a Canadian foreign intelligence agency, with but a fraction of their resources, predict such an attack or significantly supplement the intelligence produced by the Americans? Critics add that, even if Canada were to create a foreign intelligence service, years would be needed to establish networks and even longer for them to produce usable intelligence. What benefit would Canada gain from such an agency, given its costs, when the United States and Canada share over eighty treaty-level defence agreements and 250 memoranda of understanding on defence and intelligence matters? There are other questions that need to be answered as well: How would it be organized? What would be the focus of a CFIS? What would it do to Canada’s self-

perception in international affairs as being an impeccably honest broker if it were known that there were Canadian spies abroad? What about oversight? Where possible, these questions are addressed in the course of this argument. Even counterfactuals, for which no answers are available, have the merit of focusing our attention on the more fundamental issue: why Canada lacks spies and why this is not in the country's national interest.

Notwithstanding the reluctance of Canadians to fund its military and security organizations at a suitable level and the preference to avoid facing the realities of international politics that makes the symbolism of an honest broker both naïve and mendacious, the question of creating a foreign intelligence service has not gone away. In response to the answers (discussed below) provided by RCMP Commissioner Giuliano Zaccardelli and by CSIS Director Ward Elcock to a parliamentary committee responsible for security oversight (the Security Intelligence Review Committee – SIRC), several interested parties have speculated about whether CSIS has, in fact, operated as a foreign intelligence agency without an explicit mandate authorizing it to do so.² This is an important question because CSIS is, by definition, mandated to collect and analyze only “security intelligence,” that is, to undertake only domestic operations against subversive threats. As indicated, the term “foreign intelligence” refers to intelligence collected abroad and accordingly is directly tied to Canadian foreign policy. The distinction is fundamental.

Whatever the legality of the existing CSIS acting like the not-yet-existing CFIS, the chief concern of this paper is to analyze the issues surrounding the establishment of a Canadian Foreign Intelligence Service. As we shall see, there are plenty of opportunities to reflect on the consequences of not establishing one. If, as John Le Carré once observed, secret services reveal the deeper character of the countries they protect, so too does the absence of such protection. To speak personally, the question that I initially found perplexing is this: Why on earth do Canadians think they can flourish, perhaps even survive, without spies? What national character flaw leads us to think we are so exceptional? This is, of course, a very large question, and the answer, if there is one, is not self-evident. A more manageable one, discussed in the following section, is, When did Canadians start thinking this way?

One thing does seem clear: Canadian reluctance to spying is not simply a common difficulty that democracies have in hiding the ends pursued by governments from their citizens. After all, other democracies have found a use for foreign intelligence services and have organized them in a way that does not pose a threat to the regime. Yet there is always something clandestine and troubling about intelligence gathering. Surveillance, for example, cannot be done except secretly. As noted, secrets must be stolen. By the same token, covert action (action hidden from citizens by their government) is nearly always counterproductive in a democracy. There may be no easy way, perhaps no way at all, to square the circle of democratic governments using spies. But in a democracy, even that dilemma needs to be understood. Although citizens may be unaware of what is being done in their name, it is nevertheless important for them to know that something is being done. Doing nothing when others are doing things to you is politically inexcusable.

² See MacCharles 2004; Wark 2003; Travers 2004; CTV 2004; CP 2004; Bronskill 2004; Sears 2004; Brown 2001; Ross 2004; McClintock 2004; Chwialkowska 2001; and Mofina 2001.

2. THE HISTORY OF CANADIAN FOREIGN INTELLIGENCE

2 (a) Origins

Canada got into the intelligence business shortly after Confederation. Even prior to 1867, however, the British North American colonies were targeted by Fenian raiders, Irish-American terrorists who hoped to destabilize British rule in Ireland by attacking the British Empire in North America. Prior to Confederation, Gilbert McMicken led a clandestine service of twenty-five men to Buffalo and Detroit on a mission to gather intelligence on local Fenian movements (Senior 1991, 42–43). The new government of Sir John A. Macdonald developed a system of early warning and surveillance against the Fenians located chiefly in east coast American cities (Wark 1989, 78). In March of 1866, the Roberts wing of the Fenian Brotherhood circulated a rumour that an invasion of Toronto was imminent. The government took the threat seriously enough to call up volunteers to protect the frontier, at least partly as a result of intelligence gathered by a rudimentary and somewhat amateur organization established previously to counter Confederate sympathizers in Canada who were supporting military operations against the American federal government during the American Civil War (Senior 1991). To deal with the Fenian threat, Macdonald created two separate intelligence organizations, one for domestic intelligence gathering, particularly in Toronto, and another operating in the American Midwest. The British consul in New York also collected intelligence on the Fenians that was then regularly forwarded to Canada. Moreover, Thomas D'Arcy McGee, one of the Fathers of Confederation and a minister in Macdonald's cabinet, induced Macdonald to send special agent R. N. Scott on a spy mission to New York to investigate the Fenians. By late 1866, Macdonald was employing three rings of agents in Canada and the United States. In 1868, when a Fenian assassinated McGee, Macdonald asked McMicken to organize the new Dominion Police. Its immediate tasks were to monitor and infiltrate the Fenian movement and protect cabinet ministers, but as time passed, the Dominion Police became responsible for security on Parliament Hill and most federal policing services (Mount 1993, 12). Although Macdonald had employed a number of intelligence agencies, the Dominion Police was Canada's first formally organized intelligence agency.

The decline of the Fenian threat eliminated the need for spies in America. The Dominion Police and the Royal North-West Mounted Police did not send their members outside Canada to collect intelligence, despite the precedents for such action, namely McMicken's having posted Canadian intelligence agents to Chicago and Cincinnati in 1866. However, after the Dominion Police Force was formed, the government saw no justification to send Canadian agents into foreign parts and argued on grounds that have since become second nature: our chief ally, in this case Great Britain, could monitor potentially hostile activities abroad, including at this time the United States. Accordingly, as the direct threat to Canada posed by the Fenians vanished, so too did Canadian foreign intelligence capabilities. Thus began, shortly after Confederation, the tradition of Canadian police and intelligence services obtaining their material from allied sources.

2 (b) The Great War

With the exception of modest liaison contacts with the Indian government regarding Sikh revolutionary movements in British Columbia during 1912–14, the Government of Canada remained unconcerned with intelligence until the outbreak of war in 1914, when for the first time Canadians were exposed to the realities of subversive activities taking place on Canadian soil. At the outset of hostilities, internal security in Canada was decentralized and uncoordinated. Under the War Measures Act, the Dominion Police were supervised by the minister of justice, but in the

west, the Royal North-West Mounted Police were the responsibility of the Privy Council. Good detective work, vigilance, and luck restricted the damage inflicted by Germans and German-Americans. British intelligence, counter-intelligence, and counter-subversion operations in the United States were part of the reason for the limited success of the German agents, but their operational clumsiness also helped expose conspiracies directed from the German embassy in Washington against targets both in the United States and in Canada. This brought German spies to the attention of Canadian, American, and British intelligence organizations (Mount 1993). During the war, Canada's modest intelligence capabilities served the Allied war effort rather than national intelligence needs, and Canadian foreign intelligence capability remained tightly bound to, and dependent on, British and American organizations. The Dominion Police assumed responsibility for internal security and counter-subversion and relied on foreign police and military agencies, particularly the Pinkerton Detective Agency and the British military, to furnish foreign intelligence. Most intelligence doctrine used in Canada during this time was a faithful copy of the British original.

The chief lesson concerning collection, analysis, and production of intelligence was derived from the experience of war-fighting as a member of an alliance (Wark 1989). Canada's military contribution to the Allied war effort brought an increased flow of information from London, which was sustained beyond the end of the war. The American entry into the war in 1917 introduced a new dynamic to the Canadian intelligence community, necessitating new connections between London and Washington and between Ottawa and Washington. At the same time, it was clear that Canada was a junior partner within the British Imperial and Allied intelligence systems so that, in effect, Canadian intelligence evolved in the context of a foreign war fought by the Allies, especially by Britain.

The pattern of Canada's geopolitical emergence into the modern intelligence world, established during the Confederation period, was confirmed: Canada would depend on allies for foreign intelligence. This was, said Mount, "understandable" and even "fortunate," inasmuch as Canada was remote from the trouble spots of the world and usually understood its interests as being close to, if not identical with, those of Great Britain. At the same time as it was apparently a benefit to receive so much intelligence at so little cost, it was "not something on which subsequent generations could continue to rely" (Mount 1993, 24). And yet they did.

2 (c) Inter-war Years

During the inter-war years, the intelligence community in Canada suffered from the same neglect as the military. Defence and security budgets were small, and the government offered little guidance as to what Canadian strategy or doctrine should be. Military intelligence returned to pre-1914 levels of manning and status. Internal security matters received only sporadic attention, particularly after the danger posed by the Winnipeg General Strike of 1919 had passed. During the inter-war period, the wholesale reliance on British military organization and doctrinal guidance stunted the growth of a thoughtful and critical military profession in Canada. Intelligence was no exception (Steven 1988). Only the continuing injection of strategic information from London and elsewhere in the British Empire kept these modest Canadian intelligence organs alive. Indeed, Imperial intelligence was effectively the only intelligence product available to Canada, because no Canadian agency was dedicated to collecting foreign intelligence.

Internal security created separate concerns in Canada during the inter-war period. Roughly a third of the settlers who arrived in Canada between 1896 and 1914 were from continental Europe, including Ukraine and Russia. With the communist victory in Russia in 1917, priority for internal

security operations focused on potential communist subversion within the émigré community and the growing ranks of the socialist movement. When the War Measures Act was passed in 1914, immigrants from countries such as the German and Austro-Hungarian Empires, and later Russia and Ukraine, were interned and investigated. Radical left-wing activity within Canada mushroomed after 1917, inspired by the Bolshevik Revolution in Russia and by growing labour militancy. The government of the day saw this as a threat to the stability of parliamentary democracy and accordingly increased internal or domestic security intelligence operations.

During and after World War I, security intelligence resources were allocated to countering the communist threat rather than to foreign intelligence collection or even liaison. The experience of the First World War and the growing fears of subversion reinforced the need for a single national police force. When the new RCMP came into existence in 1920, its attitudes towards security and intelligence had already been shaped by the RNWMP, which had gained experience running agents in Alberta and British Columbia during World War I (Kealy 1993). The fledgling RCMP took the position that the threat of communism was entirely domestic, and following the end of the war, developed an extensive undercover, anti-subversion capability (Cleroux 1989a). Not surprisingly, the RCMP viewed the Communist Party in a criminal context. Thus the federal police aimed to stop communist activities, arrest the perpetrators, and gain convictions and legal redress, rather than attempt to undermine or control their activities, which would have meant employing classic counter-intelligence tactics (Sawatsky 1980, 65).

After 1920, the RCMP took over from the Dominion Police the direct relationship established with British security officials and began reporting directly to London. Later that year, Charles Hamilton was appointed the first and only RCMP officer to hold the post of liaison and intelligence officer (Kealy 1993). He worked directly for the RCMP commissioner and had frequent contact with Scotland Yard. This gave Canada direct access to intelligence on communism from British sources, which were more extensive at the time than those in North America. RCMP security bulletins during the inter-war period outline an extensive liaison between the RCMP and British intelligence focusing on communist activity in Canada (Kealy and Whitaker 1993). Little mention was made of American intelligence, and a formal relationship with the United States did not begin until 1937 (Kealy 1993).

2 (d) World War II

Canada received and acted on excellent tactical intelligence during World War I, but not until the Second World War did the country develop a broad and effective military intelligence organization. As a result of the Treaty and Statute of Westminster in 1931, Canada became a fully sovereign country in law. Even so, it quickly entered World War II against Germany as an ally of Britain and initially directed its intelligence efforts towards meeting British needs rather than acquiring information directly relevant to Canadian security. Moreover, even though the size of Canada's military contribution to Allied forces was unprecedented, and even though Canadians fought in independent national formations, the political and military leadership of the country was entirely dependent upon its allies for strategic assessments of both the European and the Far Eastern theatres. Initially the intelligence came only from Britain, but it later came from the United States as well (Wark 1989).

During World War II, internal security and counter-subversion were the responsibility of the RCMP. When Germany invaded the USSR in 1941, the Soviet Union became an ally of Canada and Britain, and concerns about communist subversion were considered less important than the threat of Nazi espionage, thus the RCMP concentrated on fascist elements in Canada almost to

the exclusion of its former communist targets, although communist intelligence agencies continued to target Canada. Unfortunately, the RCMP uncovered little evidence of this activity at the time (Sawatsky 1980).

The fall of France in spring 1940 and the possibility of an invasion of England presented Canada with its first major security threat (Sokolsky 1989). Thus began the well documented shift away from the United Kingdom and towards the United States as Canada's chief ally. The 1940 Ogdensburg Treaty formalized the means and methods to coordinate North American security and information sharing. United States/Canadian intelligence co-operation began in October 1941 when the Canadians offered the United States Federal Communications Commission free access to the product of Canadian wireless monitoring activities. In return, the United States gave Canada technical direction-finding (DF) data that subsequently made significant contributions to the Allied North Atlantic Ocean surveillance network. This was the beginning of Canadian SIGINT capability, which has survived into the present.

The Canadian code-breaking agency was also successful in intercepting and decoding German espionage control messages to and from agents in South America, Canada, Hamburg, and Lisbon. By virtue of its geography, Canada was well located for SIGINT operations, which is the main reason why the country became involved in the Allied and great-power intelligence alliance, and why the foreign intelligence product collected was chiefly SIGINT rather than human intelligence. Moreover, its quality and importance was defined only by how it met the needs of the coalition. With one exception, Canadian HUMINT activities were confined throughout the war to providing administrative, operational, and individual support for British human intelligence activities (Stafford 1986).

The exception to the Canadian tradition of avoiding the difficulties and ambiguities of spying and collecting HUMINT was "Camp X". This facility, built near Whitby, Ontario, opened for business the day before the Japanese attack on Pearl Harbor brought the United States into the war. It was part of a complex intelligence-sharing and counter-intelligence training program brokered by William Stephenson, the legendary INTREPID, between British MI6 and the fledgling American Office of Strategic Services (OSS) run by General William Donovan. After the war, the OSS became the Central Intelligence Agency. In 1941, however, the Americans came to Canada to learn with Canadians how to spy and to undertake other kinds of dirty tricks from the British (Granatstein and Stafford 1990, 80–81). In short, Canada was an important element in both the support and the conduct of secret intelligence activities during World War II. Many RCMP officers, CIA agents, and Canadian spies received instruction at Camp X, both in the black arts of subversion and espionage as well as the more familiar defensive techniques of counter-espionage and counter-intelligence (Lynn-Philip 2002). It is important to recall that Canadians were as immersed in the nasty business of spying as their allies because of the post-war attitudes of senior officials, chiefly in external affairs, who claimed that, somehow, Canadians were above such things.

During the war, at the request of the undersecretary for external affairs Norman Robertson, the National Research Council established an examination unit to spy on the Vichy French legation because Vichy "was suspected of propaganda activities in Quebec." Lester Pearson, T. A. Stone, George Glazebrook, and Robertson were all kept informed of the secret intelligence acquired by the examination unit. Mackenzie King, in contrast, ensured he was not informed so he could not answer if asked. "Nothing was written down. Intelligence," said Glazebrook, "is handled like no other subject. It is purely personal and almost entirely oral" (Granatstein 1981, 180). Such extraordinary secrecy was not undertaken to protect French sensibilities but because the allegiance of Quebec to the prosecution of the war was so delicate. By February 1945, the future of the examination unit, or of anything like it, had already become doubtful.

2 (e) No Foreign Intelligence Service for Post-war Canada

The question of the post-war architecture of Canadian intelligence was first raised in 1942. The Canadian Joint Intelligence Committee (CJIC) had been established to coordinate intelligence and conduct liaison with Britain and the United States. CJIC was looking for a role in peacetime and saw itself as the natural body to organize and direct future Canadian intelligence operations, both security and foreign intelligence. Gilbert Robinson of the University of Toronto, who had worked on breaking German codes during the war, advised Robertson in November of 1944 that

the world will be a troubled place for a long time to come, and there will undoubtedly be countries in whose activities we shall be particularly interested ... Canada has been led to a window on world diplomacy which, otherwise, she might never have looked through. Whatever is decided concerning this office, most countries of the world will continue doing cryptographic work after the war is over and I cannot agree that Canada will improve her position in world affairs by renouncing all activity in this work. (quoted in Granatstein and Stafford 1990, 38)

About a year later, the CJIC produced a detailed memorandum, "Foreign Intelligence in Peacetime," and sent it to both the military leadership and to senior management in External Affairs. It pointed out that atomic weapons placed a new priority on "monitoring scientific and industrial developments" as well as warding off any surprise attack. Dealing with both these post-war novelties demanded a robust and aggressive foreign intelligence capability. The CJIC also argued that Canada's wartime contribution required a larger post-war profile and that it simply could not revert to prewar dependence on the United Kingdom. They proposed a joint coordinating bureau of intelligence to conduct all varieties of intelligence gathering: military, political, scientific, and topographical. It would necessarily involve foreign intelligence (Wark 1989).

In December 1945, Lt. Gen. Charles Foulkes, chief of the general staff, produced "A Proposal for the Establishment of a National Intelligence Organization." In this memo to Robertson, he argued that just as good intelligence regarding one's military opponent in wartime was necessary to the success of military operations, so a wise foreign policy depended on good foreign intelligence, implying that Canada should develop a post-war foreign intelligence capability. Moreover, Foulkes went on, Canada's position as part of a North Atlantic partnership required that Canada gain access to allied intelligence and must therefore be able to make an effective contribution.

The position of Canada, in respect of defence and peace time economy, on the one hand, as a member of the British Commonwealth and, on the other, as an essential economic and military partner of the United States is a paramount political factor. This position ... indicates the need of Canada sharing the fruits of the intelligence activities of the two other Powers in keeping Canada in their confidence. At the same time, sharing on a unilateral basis is rarely productive of the best results, and if a pooling of intelligence is in the best interests of Canada, it will be enhanced by Canada's making a contribution to the pool. It follows, therefore, that Canada's organization for intelligence should be such as to hold the respect and free confidence of her partners in world affairs. (quoted in Wark 1989, 88-89)

Foulkes' proposal, in short, was for a balanced but effective agency both to collect foreign intelligence and to protect domestic secrets. There was no thought of simply turning into an intelligence consumer or a free-rider. This was not simply a matter of self-respect; it reflected a shrewd understanding, based on wartime experience as a significant member of a successful

military coalition, of how alliances, including intelligence alliances, worked. In 1945, Canadians, at least in the military, had no desire to become dependent on anyone, even their closest friends.

In the event, Canada did not follow its allies in establishing a foreign intelligence service. Alistair Hensler, a former director general of operations at CSIS, suggested that two key personalities shaped the decision not to follow the American and British examples: Robertson and Glazebrook (Hensler 1995, 17–18). During the war, Robertson assumed personal responsibility for foreign intelligence, but with nothing written down, as Glazebrook said, there was no institutional memory external to Robertson's memory and no formal structures to manage intelligence flow. On some issues, he maintained an arm's length relationship from foreign intelligence because he knew Mackenzie King's ignorance of, and limited tolerance for, the subject. Instead, a Toronto businessman, Thomas Drew-Brook of British Security Coordination, became the principal British intelligence contact in Canada, even though the latter was based in New York. Drew-Brook informed Robertson regularly about his activities, but as time passed, the regularity of this contact waned. It is unclear what foreign intelligence matters Robertson dealt with personally, although Drew-Brook, who operated outside the government and who had no decision-making authority within it, coordinated much of the operational support for British foreign intelligence in Canada. (Incidentally, Jack Granatstein, Robertson's biographer, was given access to all files, "except those relating to security and intelligence questions," so that the open documentary record is thin [Granatstein 1981, xiv, 168]). As a result, no one in the post-war government outside the mandarins in External Affairs knew or understood the full extent of Canadian support of foreign intelligence operations or developed an appreciation of its potential benefits (Hensler 1995, 19). Not until many years later was the espionage training at Camp X even acknowledged.

In contrast to Robertson, George Glazebrook confined his experience and knowledge of intelligence to communications intercepts and had little involvement with foreign human intelligence. Even that more sanitized experience evidently caused Glazebrook to develop a singular distaste for spying in general. While he was quick to support a continuation of Canada's communications intercept activities, he regarded other aspects of foreign intelligence as purely wartime expedients and was adamant that Canada could not afford the necessary commitment of resources to contribute anything to the work done by British Secret Intelligence Service or by CIA. According to Starnes, Glazebrook approached security and intelligence matters as "an irresistible intellectual challenge," as is, perhaps, inevitable for an academic in the spy business. Partly as a result of his approach, he was not universally admired by the military, and he reciprocated by thinking they were not very bright, "which made for uneasy relations between External Affairs and National Defence" (Starnes 1998, 84).

When External Affairs and National Defence did get together at meetings of the Joint Intelligence Committee, the chairmanship was in the hands of the military. Glazebrook represented External. In 1946, the chairmanship passed permanently to External. There is "no written record" of why this happened, though Starnes is of the opinion that it happened simply because Robertson insisted (Starnes 1998, 95). According to Granatstein, Robertson wanted post-war Canada to support only a security intelligence capability, and he preferred that it be internal to the civilian ministries, with the Privy Council Office acting as a coordinating committee along British lines (absent, of course, any Canadian equivalent of MI6). "The intent," said Granatstein, "was clearly to keep security questions close by the Department of External Affairs and as far away from National Defence as possible. The suggestion of Privy Council Office control did that" (Granatstein 1981, 181).

There was a division, therefore, between the clear-eyed military who saw the benefit of a dedicated foreign intelligence service, and the distinguished "Ottawa men" who did not (Granatstein 1998). Even Sir William Stephenson, who served the Allied intelligence effort

during World War II, was unable to persuade Canadian officials to establish a foreign intelligence collection agency. He visited Ottawa and met with Lester Pearson, then undersecretary for external affairs (Robertson by then was high commissioner in London), who was unmoved by Stephenson's argument. Alistair Hensler summarized the result: "Canada therefore entered the post-war period unconvinced of the need for a foreign intelligence service ... Unlike their American and British counterparts, Canadian policy makers were unable or unwilling to conceptualize the role of a foreign intelligence service in a period of relative peace" (Hensler 1995, 20). The reason seems to be that Robertson and Glazebrook, two men whose personal distaste for spying and idiosyncratic opinions about the importance of foreign intelligence, were tasked with planning and developing the post-war Canadian intelligence community. As to *why* they held those views, the biographic record is regrettably silent. The consequence, however, is clear: No spies for Canada.

As a postscript to this fateful post-war decision, Starnes reported an encounter in the mid-1950s with Robertson. Starnes was, at the time, the liaison officer in External tasked with coordinating business with the military. Ralph Harry, the head of the newly established Australian Secret Intelligence Service, raised the issue of the desirability, from an Australian perspective, of a Canadian foreign or secret intelligence service. Starnes took the message to Robertson "reluctantly." When Starnes spoke to Robertson, "he gave one of his huge sighs and looked at me rather reproachfully, but said nothing. He had decided to refuse the proposal, but so far as I know, it never was recorded – not by him and certainly not by me" (Starnes 1998, xi).

Finally in 1958, Robertson wrote about the need to review Canadian intelligence services. He wanted to create a "National Intelligence Body" to coordinate intelligence across all government departments. He did not, however, propose an offensive, foreign intelligence body such as CIA because "the coordination of intelligence through the creation of a new agency here [in Washington, where Robertson was serving as Canadian ambassador] has caused as many difficulties as it has solved." Moreover, it has taken a decade for CIA to get to the point where it "has approached the performance of its statutory role" (Granatstein 1981, 331). Besides, he continued, a central agency works better under the American system of government, and it was difficult for him to see how such an agency could operate outside a particular government department. Again he advocated the creation of an interdepartmental committee chaired by the Department of External Affairs. At the height of the Cold War, Robertson exemplified the questionable virtue of consistency along with unquestionable loyalty to "his" department, External Affairs.

In contrast to the withdrawal of Canada from the human intelligence field, the one area where the wartime intelligence relationship between Canada and its major allies was continued, formalized, and enhanced was SIGINT. The basis for post-war arrangements was laid during the war. In mid-1941, the British had broken the German naval Enigma code and began sharing decrypts with the United States, which in turn provided naval escorts for British and Canadian Atlantic convoys. Shortly after Pearl Harbor, the Germans began using a new Enigma variant which remained unbroken until the end of 1942. Canada joined the Anglo-American SIGINT alliance in May 1943, at the height of the Battle of the Atlantic. At the end of the war, British and American officials sought to continue what had been a successful SIGINT alliance, and by early 1946, the four main participants, the United States, the United Kingdom, Canada, and Australia had agreed to negotiate a post-war agreement (Rudner 2001, 99–103; Ratcliff 2006). Canada and Australia agreed to allow Britain to negotiate on their behalf.

The result was an agreement of around twenty-five pages known as the UKUSA Agreement, the UK-USA Security Agreement, or simply as the Secret Treaty. Large parts of it are still classified (Andrew 1994; Richelson 1999, chap. 12; Rudner 2004). The final agreement was signed in 1948

and today involves some fifteen states. From the start, the United States was and remains the dominant partner, chiefly because the National Security Agency (NSA – the chief SIGINT organization in the U.S.), dominates its allies by sheer technical superiority (Bamford 2002). The primary purpose of the original agreement was to divide SIGINT collection among the co-operating parties. Canada's responsibility was for the polar region of the Soviet Union, clearly a part of the globe of great interest to the Western allies during the Cold War (Mellon 2001). The accession of Canada to UKUSA both determined the allocation of Canadian SIGINT resources and gave the country access to information it otherwise would not obtain. Like other policy decisions, it involved a trade off. During the 1970s, the Communications Security Establishment (CSE), Canada's SIGINT agency, with help and encouragement from the American NSA, began external interception operations from Canadian embassies abroad. CSE has occasionally intercepted domestic SIGINT in other countries at the behest of domestic signals intelligence agencies that are prohibited by their own laws from eavesdropping on their own citizens (Frost and Gratton 1994, 183, 191; Rudner 2001, 107).

In contrast to the operational existence of a foreign SIGINT capability, which made trade offs at least possible, the absence of any post-war foreign human intelligence capacity was simply a net loss. From the attitudes of senior mandarins and the even more negative opinion of Prime Minister King, there developed the peculiar, but soon to become typical, attitude in External Affairs (which has been carried over to DFAIT) that somehow spying is not the Canadian way and that, if ever Canada did create a CFIS, it would sully an otherwise pristine reputation (Mellon 2003, 8). Such an attitude is, to say the least, naïve, because no country chooses its enemies; enemies choose it. As William S. Stephenson (not INTREPID) pointed out, it was, in fact, much worse than naïve; it was stupid.

The easy way out is to pretend there are no crises. That's the way to win elections. That's the way we stumble into war in the first place – there were too many men in power who preferred to see no threat to freedom because to admit to such a threat implies a willingness to accept sacrifice to combat it. There's a considerable difference between being high-minded and soft-headed.
(Stephenson 1999, 511)

This self-serving mendacity regarding Canadian attitudes towards foreign policy realism has not waned over the years (Cooper 2004a). It is not, however, some kind of "Canadian disease." In 1930, Herbert Hoover's newly appointed secretary of state Henry Stimson decreed that the "Black Chamber," which analyzed foreign codes and ciphers, was to be disbanded. According to Stimson, "gentlemen don't read other gentlemen's mail" (Codevilla 1992, 133). The Black Chamber was immediately reborn as the Army Signal Intelligence Service, a fact that was not shared with the State Department (Bamford 2002, 3). The Canadian military was not so imaginative.

One of the reasons for this reluctance was no doubt the acceptance by the military of civilian control. Another lay in the faulty assumption behind General Foulkes' 1945 memo. His argument was formed on the basis of his experience of the benefits derived from Alliance co-operation in World War II and from the expectation that Canada would remain a significant power in the post-war world. The actual priorities of the Liberal government lay rather in the opposite direction and relied on the conviction that neither Britain nor the United States would permit any hostile military actions against Canada. Any attack on Canada would certainly be construed as a serious threat to the United States. It was enough that Canada was part of the UKUSA Agreement, insofar as the major signatories could (and in the opinion of the Canadian government, they would) provide all the intelligence Canada required for its own security. The CANUS Security Agreement of 1949, a secret bilateral treaty governing the exchange of SIGINT, deepened this relationship (Richelson and Ball 1990, 143). In short, the free-rider sentiments that later

characterized so much of Canadian post-Cold War defence and security policy began shortly after the end of the Second World War in the area of intelligence policy. The Canadian government seemed oblivious to the risk it was taking, namely that without an effective security intelligence organization or an independent agency to gather foreign intelligence abroad, Canada would become a soft target for other hostile intelligence agencies, above all KGB and GRU (Soviet military intelligence). This vulnerability was exposed soon enough with a spectacular “walk-in” source of human intelligence, the defection of Soviet cypher clerk Igor Gouzenko in 1945 (Bothwell 1998; Zubock and Pleshakov 1996).

2 (f) Post-war Counter-intelligence

Foulkes’ memo did not contain any hint of the approach of the Cold War. When Gouzenko’s documents indicated the existence of extensive networks of Soviet agents operating in Canada during the war, the government was shocked (Granatstein and Bothwell 1982). Robertson in particular was both pained and surprised that Canadian civil servants would betray their country – all the more so because he was well acquainted with many of the people Gouzenko named (Granatstein 1981, 174; Knight 2005, 127). For his part, the prime minister “was willing to give Stalin and even the Soviet ambassador to Canada the benefit of the doubt about their involvement in espionage.” King was less charitable towards Canadian traitors, however, because he “associated spying with Jews” and believed (wrongly) that they were “Jews or have Jewish wives or [were] of Jewish descent” (Knight 2005, 113, 172).

These personal issues aside, the fact is that, during the war, “for the first time ever, there was secret information in Canada that could interest another country,” information that was related to work on radar, high explosives, and the atomic bomb. After 1942, the Soviets directed most of their attention towards the atomic bomb, although not until 1944 was a separate directorate in KGB established for monitoring all nuclear projects (Sudoplatov and Sudoplatov 1994, 184). That is, a network of Soviet agents existed in Canada before Stalin made atomic-bomb information the number one priority for Soviet intelligence. When the Soviet focus then shifted to A-bomb espionage, they were in a position to exploit aggressively an organization that had been in place for several years. Because of the 1941 Hyde Park Agreement that allowed for the free exchange of war materiel and of some secret information, Canada was a target. The Soviets were interested, and GRU controllers in Canada had the assets required to begin collecting atomic intelligence (Granatstein and Stafford 1990, 48).

In June 1943, Colonel Nikolai Zabolotin arrived in Canada as the new Soviet military attaché, although his chief task had little to do with his official post. Zabolotin’s assignment was to strengthen the network of GRU spy rings in Canada. Some years before, when Russia had no diplomatic mission in Canada, Soviet intelligence agents operating from across the border in the United States had established the beginnings of a spy network in Canada. Upon his arrival, Zabolotin assumed control of two main networks headed by leaders of the Communist Party of Canada (CPC): Fred Rose, MP, and Sam Carr. Rose was born in Poland, emigrated to Canada and later studied political subversion at the Lenin School in Moscow. When he returned to Canada, he joined the CPC and was handled by Zabolotin. Carr, a Ukrainian émigré, also attended the Lenin School and joined the CPC upon his return (Noel-Baker 1955, 64–80).

The recruitment of Canadian spies was effective, starting with the two senior agents recruited from the ranks of the CPC. When Zabolotin sought to expand his espionage operations, one of his priorities was to recruit people willing to supply secret information. He determined that the people most likely to co-operate were those who believed in, were sympathetic with, or

susceptible to, Communist ideology. Ideologically seduced, contaminated, or infatuated, such people were the most unlikely to denounce him to unwitting Canadian authorities. Most Canadians who joined this espionage network were well educated and were regarded as agents of marked ability and native intelligence. That respectable citizens could be traitors demonstrates, among other things, the care with which they were selected by the Soviets. Similar expertise was developed in the United Kingdom and the United States. As the Royal Commission on Espionage, created in response to Gouzenko's revelations, noted:

[t]he way in which some persons who were in a position to furnish secret information, or who might be used as contacts and who had inherent weaknesses which might be exploited, were selected and studied, clearly establishes this. The methods of approach varied with the person and the position. (Canada 1946, 43)

The Soviets had several advantages in developing their wartime Canadian networks. At that time, the main intelligence threat was perceived to be from Nazi Germany, not from the Soviets. Consequently, as noted, the RCMP focused on Nazis rather than Communists. When Zabolotin arrived in Canada, he had agents in place and he could also recruit new agents in comparative safety, because Canadian security intelligence resources were directed elsewhere. When his chief target became atomic intelligence in 1945, Zabolotin's network was well placed to supply sensitive military and political information. Without an effective security intelligence agency or foreign intelligence service to gather counter-intelligence on Soviet activities, Canada proved to be relatively easy pickings for an effective Soviet espionage operation. Given the ability of the Soviets to penetrate British and American agencies, there is, of course, no guarantee they would not have done the same to Canada even if the country had an effective foreign and counter-intelligence capability. But lacking both, Canada was that much more vulnerable.

Following the 1946 Royal Commission on Espionage, the top priorities of the government quickly became domestic intelligence (security intelligence) and signals intelligence. The RCMP assumed responsibility for internal security and security screening. In addition to provincial contract-policing and federal policing duties, it quickly became deluged in security clearances and investigations. With an internal security system energized by Gouzenko's revelations, Canada ignored foreign intelligence, trusting that intelligence-sharing agreements with its allies would provide what was needed. In fact, however, the RCMP was neither equipped nor trained to handle the major counter-spy operation that Gouzenko's information would have required. Accordingly, the British and Americans were soon called in (Sawatsky 1980, 93). While the RCMP was nominally responsible for internal security, after Gouzenko's revelations, they realized that their limited security intelligence capabilities had to be expanded. The entire RCMP Intelligence Branch consisted of roughly twenty-four officers, too small even to monitor regularly the Soviet embassy in Ottawa. No attempt was made to turn any of the Canadians exposed by Gouzenko into double agents, chiefly because the RCMP had little experience with serious espionage and counter-intelligence. In 1946, the RCMP established a "Special Branch" within the larger Criminal Investigations Section. It was staffed with individuals dedicated to counter-espionage and intelligence gathering, and included units specializing in surveillance, from which eventually emerged the RCMP Watcher Section (Cleroux 1989a, 35). As the Cold War escalated, the RCMP came under increasing pressure to expand their internal security intelligence operations.

Foulkes' recommendation in his 1945 memo for a Canadian Joint Intelligence Bureau (CJIB) was eventually adopted, but too late "to use intelligence resources and to establish effective liaison with the new Central Intelligence Agency in the United States and with a restructured British intelligence service" (Wark 1989, 90). By the time the CJIB received funding and orders in 1948, its mandate had been changed (no doubt as a result of Robertson's prior influence) towards

obtaining domestic economic intelligence and mapping the north. There was no concern with recovering, creating, or maintaining an intelligence organization capable of handling a wide range of intelligence tasks. Nor was there any concern to develop an independent capability in a specialized area of signals intelligence, where Canada excelled during the war, in order to develop a significant quid pro quo for Canadian participation in the North-Atlantic partnership under the UKUSA Agreement. Even in the area of Canadian strength, namely SIGINT, opportunities were lost.

One result of the Gouzenko affair was that Canadian intelligence collection grew even more secret. The modest continuation of signals intelligence was officially denied existence. The Communications Branch of the National Research Council was eventually renamed the Communications Security Establishment (CSE) in 1975. Both, however, were created by order-in-council, and not until the creation of the Department of Public Safety and Emergency Preparedness in 2001 was the CSE given a statutory foundation. As with NSA in the United States, for many years its initials were also officially secret. In addition, because Canada is a net consumer of intelligence, the bureaucracy has had to be even more secure and thus more secretive than the intelligence producers. Thus, in some instances, it is easier to obtain information from Washington about Canadian activities than it is from Ottawa.

Meanwhile, in the area of security intelligence, Special Branch was upgraded in 1956 to the status of Directorate of Security and Intelligence. It targeted a number of institutions and searched for suspected communist subversion. The Canadian Broadcasting Corporation (CBC) was one of the most vulnerable targets and one of the first to be investigated (Sawatsky 1980, 112). Within months, aggressive checks into the loyalty of CBC staff were undertaken, particularly of on-air personalities who were in a position to indoctrinate Canadians with communist propaganda. In 1949, the National Film Board was refused a contract with the Department of National Defence because of Gouzenko's allegations that communist sympathizers existed within it. After Gouzenko, however, ideological spies were hard to find because the Communist Party of Canada was too closely watched. Civil servants considered vulnerable to blackmail included the usual suspects: alcoholics, compulsive gamblers, large debtors, and homosexuals. The RCMP later formed an investigative unit called A-3 which concentrated exclusively on homosexuals and utilized a polygraph-type instrument known informally to its operators as the "Fruit Machine." It is probably fair to say that the RCMP might have used its talents in the area of domestic intelligence production in better ways.

As early as 1955, Mark McClung, an analyst with Special Branch, urged the establishment of a separate, civilian security intelligence organization called the Canadian Security Intelligence Organization to handle counter-espionage and counter-terrorism (Sawatsky 1980, 36). He stated that the duties and practices of police and security agencies were fundamentally incompatible and Special Branch should be split, creating a civilian agency responsible for counter-espionage and foreign liaison. Unfortunately, McClung's ideas were too radical for the RCMP at the time, and the idea was ignored for over a decade.

The long-term consequence of the Gouzenko case was to fragment the Canadian security system, to skew its focus towards internal security intelligence, to isolate foreign signals intelligence, and to prevent almost to this day any serious and sustained debate over Canada's intelligence requirements. The result was "an inevitable muddle and compromise" (Wark 1989, 91). Until the mid-1960s, the security intelligence activities of the RCMP attracted almost no attention.

2 (g) The Birth of CSIS

What brought RCMP security intelligence to light was the animosity between John Diefenbaker and Lester Pearson in the politically acerbic circumstances created by minority governments. In 1966, Diefenbaker relentlessly criticized the Pearson government for their handling of the case of George Victor Spencer, a Vancouver post office employee accused by the RCMP (but never charged) with being a Soviet spy. Up to that time, there had been a gentleman's agreement not to debate security matters in public in the House of Commons. In response to Diefenbaker's break with precedent, liberal justice minister Lucien Cardin replied by leaking information for the first time in public about the heretofore secret case of Gerda Munsinger, a German prostitute with ties to Soviet agents who had done business with Pierre Sevigny, the associate minister of defence in the previous Diefenbaker government, and other ministers. In response, Pearson appointed a Royal Commission on Security in 1966 under the chairmanship of Maxwell MacKenzie.

In his report issued a couple of years later, MacKenzie recommended that a civilian security agency be established for two reasons. First, a law enforcement body should not be involved in security intelligence, because on occasion, it might be necessary to break the law when carrying out its tasks, which would be highly improper for sworn peace officials. Secondly, RCMP Special Branch lacked "sufficient sophistication and powers of analysis" to do security intelligence work (Rosen 2000, 3). The MacKenzie Commission also recommended that the use of "intrusive investigative techniques" – that is, breaking and entering – be legalized for security intelligence operatives.

In 1969, Prime Minister Trudeau said it was time "to participate in a full and informed discussion of security matters," but Robert Stanfield responded that "the fact is that on matters relating to our national security, Parliament has always accepted some considerable limit on its right to demand information and full disclosure by government" (Canada 1969, 10636, 10638). As a result, there was no debate and no discussion of the desirability either of a civilian security intelligence agency or of a foreign intelligence agency. The Trudeau government, in fact, rejected the recommendation of civilianization, but as a compromise, appointed a civilian, John Starnes, to be the director general of the Security Service, which kept its counter-espionage role and its largely RCMP staff. The RCMP has been a paramilitary organization from its founding, so not surprisingly, its members strongly resisted civilianization; in 1970, there was not one civilian in an officer-equivalent position in the planning or operations offices of the Security Service. Moreover, the Security Service retained the powers of a police organization, but it was increasingly independent of anything like a police command structure. On the one hand, Parliament continued its policy of non-interference with the RCMP, which is entirely appropriate. On the other, because the Security Service acted in secrecy, the policy of non-interference was an invitation for them to act in highly questionable ways, secure in the knowledge there would be neither political nor chain-of-command oversight. In 1970, Starnes told Solicitor General George McIlraith that the RCMP had been acting illegally for two decades (Cleroux 1989a, 54; Starnes 1998, 171–87).

Under the pressure of events, chiefly the rise of Quebec separatism and the FLQ terrorist activity that eventually constituted the 1970 "October Crisis," the Trudeau government instructed the Security Service to undertake a more proactive strategy. They did. The Security Service, still with no oversight, proceeded to harass, infiltrate, disrupt, conduct surveillance, intercept mail, and obtain a great deal of intelligence by illegal and otherwise dubious means such as the use of *agents provocateurs*. Mission creep changed the target from the FLQ to all shades of nationalist opinion in Quebec; in other parts of the country, a wide variety of left-wing and radical groups were targeted. Quebec was not the only venue for illegal activity, but three of the more spectacular acts took place there: burning down a barn in order to destroy a meeting place for Quebec nationalists and American anti-Vietnam War radicals; breaking into a left-wing Montreal

news agency and destroying its files; and breaking into the headquarters of the separatist Parti Québécois to steal its membership lists (Whitaker 1988).

In 1977, the Trudeau government appointed Justice D. C. McDonald to head a commission of inquiry into allegations of wrongdoing by the RCMP. It was, as expected, highly critical of the Security Service, but it was no less critical of the politicians for their failure to exercise oversight and due diligence. As with the MacKenzie Commission before it, the McDonald Commission also noted that the RCMP had insufficient sophistication and analytical ability. As a result, the Security Service seemed incapable of distinguishing dissent (especially on the Left) from subversion.

The chief recommendation from the McDonald Commission was the proposal to create a civilian security intelligence agency separate from the RCMP. Section C of the report is entitled, “Should Canada Have a Foreign Intelligence Service?” The commission confirmed that the absence of such an agency placed Canada “in a position of considerable dependence on its allies” and constrained the success of its security intelligence organization. The commission did not, however, analyze Canada’s intelligence sharing alliances but nevertheless concluded that Canada received adequate foreign intelligence from its allies (Canada 1981, 626). In fact, it had no way to know this.

The commission also indicated the need to move away from deterring subversion and towards intelligence collection and analysis. This required new personnel, not police officers, and an organizational structure that included political oversight and review. The new agency required a statutory mandate to deal with espionage and sabotage by foreigners, political violence and terrorism, and revolutionary subversion. It would not, however, have any capability to enforce security, which was left up to the police or the military, although it could employ intrusive investigative techniques – mail-opening, wiretapping, surreptitious entry, and electronic surveillance – provided it first obtained a judicial warrant. The director general of the new agency would report to the solicitor general of Canada, and their operations would be overseen by a three-person Advisory Committee on Security and Intelligence, reporting to the minister and to Parliament. McDonald also recommended the establishment of a parliamentary oversight committee.

In May 1983, Bill C-157 was introduced with the objective of creating the Canadian Security Intelligence Service based more or less on McDonald’s recommendations. It was immediately construed as an attack on civil liberties and so widely and strongly denounced that the government referred it to a special senate committee chaired by the close friend of the prime minister, Senator Michael Pitfield, rather than proceed to second reading, which prompted Ned Franks, one of Canada’s foremost students of Parliament, to observe that “the Government has acted as though it is scared to death of Parliament, and that Members are mischievous, naughty little boys who can’t be trusted with serious issues like security” (Franks 1983–84, 338). The Senate reported back in late November with over forty recommended changes, and the bill died on the order paper.

In January 1984, a new bill, C-9, was introduced that incorporated many of the Senate recommendations. It was still opposed by the NDP, and the Tories wanted the Security Service to stay within the RCMP, but in July 1984, CSIS came into existence, along with the Security Intelligence Review Committee (SIRC) to review its activities. Section 2 incorporated the McDonald Commission definition of threats to the security of Canada noted above. Section 12 described the purpose of CSIS, to investigate, collect, analyze, and retain information on security threats; s.13 tasked the new service to provide security assessments for government employees. The act also defined the extent and limitations according to which CSIS can conduct foreign intelligence gathering. Under s.16, CSIS was restricted to collecting foreign intelligence within Canada, preventing CSIS agents from travelling abroad to collect foreign intelligence or conduct hostile operations.

2 (h) Collection of Information Concerning Foreign States and Persons

16. (1) Subject to this section, the Service may, in relation to the defence of Canada or the conduct of the international affairs of Canada, assist the Minister of National Defence or the Minister of Foreign Affairs, **within Canada**, in the collection of information or intelligence relating to the capabilities, intentions or activities of

(a) any foreign state or group of foreign states; or

(b) any person other than

(i) a Canadian citizen,

(ii) a permanent resident within the meaning of the Immigration Act, or

(iii) a corporation incorporated by or under an Act of Parliament or of the legislature of a province. (Canada, 1987)

At the same time as s.16 appears to confine CSIS to Canada, using the authority of s.12, CSIS has occasionally sent intelligence officers abroad to collect information. Former Solicitor General Pierre Blais stated in 1990 that while CSIS does not seek to conduct offensive operations abroad, it does have the power to investigate threats to Canada abroad (Canada 1990b, 39). These responsibilities are examined in detail below.

CSIS immediately experienced problems with its mandate to protect Canada from hostile foreign intelligence services within its borders. In theory, the new civilian agency would escape the police culture or “mentality.” In practice, the RCMP Security Service changed its name without changing its personnel or mindset – indeed, 95 per cent of the original CSIS agents were transfers from the RCMP Security Service (Whitaker 1988, 56). Moreover, because the new CSIS building was still under construction, the organization kept their old address at RCMP headquarters. The new civilian service was to undertake security intelligence while leaving protective security and federal policing to the RCMP. The new agency would not have police powers, nor would it carry weapons or make arrests, which also remained the exclusive task of the RCMP. The result, as might have been anticipated, was a debilitating and extended bureaucratic turf war. The RCMP, for instance, refused to allow CSIS full and direct access to the Canadian Police Information Centre, thus ensuring that CSIS had access to much less information than its predecessor, the RCMP Security Service (Cleroux 1989a, 169). Hostilities were supposed to have ended in 1989 with a secret “peace treaty” between the two organizations, though this is doubtful. The refusal or inability of the two agencies to co-operate in the investigation of the June 1985 Air India bombing or the mutual recrimination over the Maher Arar problem shows that tensions remained strong well into the new century (Mayeda 2006a, 2006b). In 2007, yet another memorandum of understanding was signed, the purpose of which was to ensure future co-operation (CASIS 2007).

As far as CSIS operations abroad are concerned, the record is not promising. Poor operational security was responsible for the loss of classified documents on at least four occasions when CSIS members removed sensitive documents from Service offices, contrary to procedure (Bronskill 1999; Cleroux 1989b). Similarly, the United States Justice Department criticized CSIS in 2001 when the Americans learned that CSIS had destroyed critical wiretap evidence implicating Ahmed Ressam, the so-called Millennium Bomber who was arrested before he could attempt to bomb Los Angeles International Airport (Duffy 2001). Again in 2001, CSIS was in the public spotlight when it was successfully sued for wrongful dismissal over the firing of a senior internal security agent (Friscolanti 2001). Simply on the grounds of such examples of incompetence it does not seem

prudent to expand CSIS mandate explicitly to include foreign intelligence. As is outlined below, there are other and more compelling reasons not to extend its mandate.

In March 2002, six months after 9/11, the RCMP announced it was boosting its liaison presence overseas, “to provide Canadian and foreign law enforcement communities with assistance, information, and coordinating support for investigations related to drugs, organized and commercial crime, and immigration matters” (Humphries 2002, A4). The RCMP has always maintained liaison personnel abroad, but the increase of liaison members in selected locations indicated that the RCMP required more foreign intelligence, which means that the sought-for information was either not collected by CSIS or it was not being shared. Either way, expanding the mandate of an already overstretched agency is a clear indication of a major problem, either with CSIS or with the absence of a genuine foreign intelligence capability.

3. THE CANADIAN FOREIGN INTELLIGENCE COMMUNITY TODAY

The patterns of Canadian intelligence created after World War II now exist in an entirely different security environment. Before the Cold War started, as noted above, Canada refused to create an external human intelligence gathering capability, relying instead on the product of its allies and placing its assets into Cold War-driven networks focusing on SIGINT. This was widely seen in retrospect as something of an anomaly. As British scholar Christopher Andrew noted, “Canada long ago decided to stop sub-contracting its diplomacy to Britain and set up its own embassies abroad. It seems curious in Britain that Canada is still willing to sub-contract its HUMINT, though not its SIGINT, to its allies” (Andrew 1991, 10). This anomalous behaviour continued after the end of the Cold War as well, as both Wark and Rudner, two academics with considerable knowledge of security questions, pointed out in testimony before parliamentary committees (Canada 2003a; Canada 2005b). According to Anthony Campbell, Canada is “one of the only countries with an international role not to have held a post-Cold War public review of foreign intelligence policy” (Campbell 2003, 158). Of course, Canada long postponed any serious review of foreign or defence policy too, so perhaps no one in DFAIT or DND saw any need to examine the foreign intelligence question.

Canada’s intelligence community today is departmentally driven. It consists of diverse groups within the federal bureaucracy having different responsibilities and capabilities for collecting, analyzing, and using foreign intelligence. The collectors include the Communications Security Establishment (CSE) and CSIS, which is responsible to Parliament through the Minister of Public Safety. Responsibility for liaisons and some collections rests with the Department of Foreign Affairs and International Trade, which is also a primary consumer of foreign intelligence. Intelligence analysis and collation occur in the Privy Council Office (PCO) and the Department of National Defence (Hensler 1999, 127). In addition, Transport Canada and the Canada Border Service Agency all have an interest in intelligence, chiefly as consumers. In terms of our present concerns, they are clearly second-tier organizations.

3 (a) Communications Security Establishment

As noted in the preceding section, the Communications Security Establishment (CSE), a civilian agency of the Department of National Defence, is the largest and most expensive Canadian intelligence organization and the chief source of foreign intelligence for the Government of Canada. It collects, analyzes, and reports on signals intelligence derived from the interception of foreign electronic and electromagnetic emissions – radio, telemetry, radar, and so on. CSE also provides advice on protecting domestic government communications and on electronic data and information security (FAS 2002; Bell 2006).

CSE analyzes and produces SIGINT. It is collected by the Canadian Forces Information Operations Group (CFIOG), formerly called the Supplementary Radio System, a military group operating under CSE direction. As part of the UKUSA community, CSE is a member of the major global SIGINT network. The chief principle of this alliance is that member countries do not target one another or one another’s nationals. In the intelligence business, the agreement not to spy on your friends is based on what was referred to above as the “friend-on-friend” principle. One reason why members exchange liaison officers is to monitor one another’s activities and verify that friend-on-friend is actually being adhered to. In conducting its operations, CSE historically obtained most of Canada’s foreign intelligence from within the context of the collaborative UKUSA alliance. However, the CSE director informed the House Standing Committee on National Security and Defence that his agency is active in Afghanistan, providing tactical

intelligence to Canadian troops on the ground (Bell 2007). With respect to the UKUSA alliance, there are clear benefits to Canada in being part of a global intelligence network, but there are obvious limitations as well, particularly as a result of a heavy dependence of the entire UKUSA network on American, space-based satellites.

Satellites facilitate global telecommunication and the interception of these same signals, both in space and by looking down on the surface of the earth and eavesdropping, for example, on microwave signals. Over the past forty years or so, American satellites captured huge amounts of information that then need to be filtered, processed, and analyzed. This entailed considerable upgrading of CSE computers during the 1980s and 1990s in order to achieve the current system of almost seamless integration of CSE with other participants in the UKUSA SIGINT community.

During the 1970s, NSA began networking UKUSA computers into a “host environment” at NSA headquarters in Fort Mead, Maryland. This hardware network, code-named “PLATFORM,” was supplemented by a software package named “ECHELON” that enabled participants to submit targets to one another’s listening posts. Since then the operational code name, ECHELON, has come to refer to the whole interception and processing system. At the centre of the enterprise are large computers referred to as “dictionaries,” programmed to search each intercepted communication – fax, email, phone call – for specific addresses, keywords, and even for voices (Goodspeed 2000). Each dictionary computer contains the designated keywords for the service operating it, but because of its networked connection to partners’ facilities, it also can access ECHELON dictionaries at other places. Thus, for example, Australia might post its search list with the Canadian ECHELON dictionary at CSE and have targeted intercepts automatically forwarded to the Defence Signals Directorate in Canberra.

ECHELON was initially designed as a genuine “all-channel” network where each participant could gain access to all the information. According to Nicky Hager, a New Zealand analyst of that country’s participation in ECHELON, it seems that participants can access only stipulated targets from their partners’ dictionaries (Hager 1996, chap. 2; Hager 1998). Rudner drew the obvious conclusion for Canadian SIGINT:

Participating organizations may request intelligence product from other partners’ “Echelon” Dictionaries, but actual access is effectively controlled by that country. If that is the case, Canada might not be able to receive output of the whole “Echelon” network even though a considerable portion of CSE’s own intelligence collection probably goes to serve other UKUSA partners requirements. It seems likely that only the NSA colossus, by virtue of its size and leadership role within “Echelon,” can access the full global potential of the system. For lesser players like CSE these controls on “Echelon” access render the reciprocal sharing of signals intelligence under UKUSA in effect asymmetrical. (Rudner 2001, 113)

The same asymmetry likely applies to orbital positioning and targeting SIGINT satellites, all of which are American. Even the project to place a Canadian craft in orbit early in 2008 is to be part of a United States Space Command network (Wattie 2004).

3 (b) Canadian Security Intelligence Service

The CSIS Act currently (2007) under review authorizes that agency to collect security and foreign intelligence, but the qualifications regarding foreign intelligence collection are unique. To review

what was noted in passing above: the primary CSIS mandate established by s.12 of the act is to collect information about threats to the security of Canada, which is a domestic concern, but without restriction on where such security intelligence can be collected, implying that CSIS can obtain domestic security intelligence abroad as well. However, its secondary mandate, the collection of intelligence about the capabilities, intentions, and activities of foreign states, is more constrained under s.16 of the act (Farson 1993, 49). The CSIS Act (quoted in s. 2 of this paper) stipulates that the collection of foreign intelligence under s.16 must take place in Canada and cannot be directed at citizens or permanent residents of Canada, even though, as just noted, CSIS sends agents abroad to conduct investigations under the authority of s.12. This odd stipulation has caused operational problems. In its 2000 report, SIRC noted that CSIS had in fact targeted Canadians while gathering foreign intelligence in Canada.

In a few instances, in the Committee's opinion, information went beyond the definition of foreign intelligence as set out in policy and law and included information that identified Canadians or gave information about their activities that had very little intelligence value. In one instance, the Service agreed and that information was removed. (Canada 2001d)

Because there is no oversight body besides SIRC, one must accept its findings that CSIS is not employing the robust techniques of foreign intelligence within Canada. As noted in section two, this was precisely the problem that led to the illegal activities of the RCMP Security Service and to its demise and replacement with CSIS.

In his 2001 testimony before the House of Commons Immigration Committee, CSIS Director Ward Elcock noted that the service conducts covert operations abroad and has a foreign intelligence mandate that is "essentially the same" as that of CIA. At the 2001 Canadian Association for Security and Intelligence Studies (CASIS) Conference, Elcock stated that his agency, "has an international mandate. [CSIS] can collect intelligence wherever [it needs] to" (Chwialkowska 2001; see also Elcock 2002a). Section 12 of the CSIS Act, as noted above, does not prevent security intelligence from being collected outside Canada. The difficulty lies, however, in drawing a line between foreign activities that are domestic and "defensive" in intent, and thus security intelligence, but offensive in operation and thus, in reality, foreign intelligence. Is the intelligence collected by an alleged CSIS covert operation foreign or security intelligence? At what point in an investigation does security intelligence begin its perilous journey down the slippery slope of semantics and become foreign intelligence? CSIS is not legally authorized to collect foreign intelligence abroad, which raises further questions: Is CSIS collecting foreign intelligence under the guise of "security intelligence," in violation of the CSIS Act? The American analogy would raise the question of whether CIA is spying on Americans at home, which is supposed to be the job of the FBI. In SIRC's *2002-03 Report*, the authors noted: "given the extremely sensitive nature of section 16 operations [foreign intelligence collection within Canada], access to the Foreign Intelligence Data Base is restricted to only those CSIS employees who have received special clearance and indoctrination. The database is thus not routinely accessible to intelligence officers involved in section 12 investigations [regarding threats relating to the security of Canada]" (Canada 2002j).

CSIS Director Ward Elcock provided an informal analysis of the question at a talk at Carleton University in June 2002 (Elcock 2002b; The direct quotes in the next two paragraphs are all from the same talk). "There is," he said, "no restriction in the act on where the service may collect information ... anywhere in Canada or – and what is more to the point – anywhere abroad." That is, indeed, a close paraphrase of the relevant provision of the CSIS Act. It is also correct, as he said, that the information so collected is "related to potential threats to the security of Canada" along with "incidentally collected intelligence which is not threat related." The use by Elcock of

the adverb “incidentally” is important because the *deliberate* collection of non-threat-related intelligence is, in fact, foreign intelligence collection, which CSIS is prohibited from doing by law. The notion of “incidental” collection of intelligence would seem to indicate something that CSIS happened upon that in their view might prove useful to the government or to law enforcement officials. By its very nature, however, it is impossible to direct CSIS to collect incidental intelligence. Accordingly, the provisions of the CSIS Act may be of little use to policymakers concerned with strategic (and thus non-incidental) initiatives.

Elcock inadvertently appeared to acknowledge the problem. Having so much riding on the adverb “incidentally” was bound to lead to what he called “misunderstandings” about the role of CSIS in “collecting intelligence outside Canada.” The reason for these misunderstandings, he said, was “because in its early years CSIS was struggling to establish an identity.” Those days of ambiguity are over. Today, after “the service has matured and developed,” they have “expanded our overseas operations progressively.” That may be so, but it is not clear whether or not CSIS is, in fact, conducting their own version of mission creep.

The issue of the ambiguity of the CSIS mission and the need to ensure safeguards were in place to keep the agency on task came up about a year later in Elcock’s 2003 testimony before the House Standing Committee on Justice and Human Rights, Subcommittee on National Security. Kevin Sorenson, Canadian Alliance MP for Crowfoot, asked: “Have there been any more discussions or any more consideration to expanding the role or expanding the abilities of CSIS to become more involved on an international stage?” (Canada 2003b). Elcock replied:

In terms of our operations abroad, it has always been within the mandate of CSIS, and it has been, if you will, an evolution in terms of the kinds of operations we run, that CSIS has the capacity and has the mandate to operate abroad. It has that mandate in respect of any threat to the security of Canada, and *inferentially*, any other information that CSIS may collect during such an investigation.

We have in the past operated and will continue in the future to operate with other agencies abroad but also to operate ourselves covertly abroad if indeed we believe there is merit in doing so in any particular case. Not every case is soluble [sic] by that kind of operation, but indeed we already do, have done in the past, and will continue to do so into the future.

Just as the use of the modifier “incidentally” was both a way of obscuring and expressing the ambiguity of Elcock’s effective understanding of the CSIS mandate, likewise the adverb “inferentially” served the same purpose, with the proviso that it was intended to convey a logical connection or at least a connection that logically might be “inferred.” A few minutes later, David Pratt, later minister of national defence in the first Martin government but at the time a backbench, Liberal M.P., asked about “gathering intelligence in other countries, foreign intelligence.” Specifically, he asked about “covert operations outside Canada” based on threats to the security of Canada, but also, “in this interconnected world of ours,” would Canada take part in operations requested by Canada’s close allies? These would be instances where Canada might be able to get information that these close allies could not, given “that when we’re talking about threats to the security of Canada, threats to the security of our allies in some respects can be, in fact, threats to the security of Canada? Is there that broad a construct that might be given to covert operations abroad?”

Elcock replied that “we do operations abroad with other organizations. We do enter into what we call joint operations with a wide variety of other agencies.” To this non-responsive response, Pratt made the obvious reply. First of all, such operations are few and limited, and second, the real

issue is the establishment of a foreign intelligence service, as Elcock knew perfectly well – not least of all because Pratt had argued for it on his website a month earlier, and on 17 March introduced a private member's bill to establish the Canadian Foreign Intelligence Agency, Bill C-409 (Canada 2003c). The fact is, as Elcock noted, that “requests from American agencies have risen 300 per cent since September 11” and yet,

unlike our allies, we've constrained ourselves by not having a foreign intelligence agency that is able to get out there and not just deal with threats to the security of Canada, but also with the myriad of other interests we may have, whether it's from a political standpoint, a military standpoint, or a commercial and economic information standpoint. We've deprived ourselves of the ability to collect that information by being the only G8 country without a foreign intelligence agency.

The solution for this deprivation was therefore obvious enough, but it was not one that Elcock was prepared to consider.

He then added that CSIS' ability to collect foreign intelligence is “not unlimited,” and that only “a huge organization” could do what Pratt suggested; besides, operations abroad “are by definition more expensive, more risky, and so on.” Thus even a dedicated foreign intelligence agency “might also be very limited and might not even exceed the number [of operations] that CSIS would do now.” It is clear (and would have been clear, at least to experienced parliamentarians like Pratt and Sorenson) that Elcock's chief concern was bureaucratic, namely to protect CSIS and prevent any serious questioning of whether Canada needs a foreign intelligence agency. Moreover, having CSIS do it all meant that “there is no gap between us and some other organization collecting outside of Canada.” And finally, if you wanted a foreign agency, Elcock estimated it would take ten or fifteen years to create and would detract from the resources given to CSIS, not a good idea during a period replete with terrorist threats.

Pratt would have known that Elcock was doing his bureaucratic duty rather than addressing the substance of the question. When it was again Pratt's turn to speak, he asked a follow-up question regarding (again) CSIS undertaking both foreign and security intelligence within the limits established by law. Pratt noted the recommendation of the McDonald Commission, discussed above, concerning the desirability of two distinct intelligence agencies, and concluded with the observation made earlier that Canada was the only G8 country without a foreign intelligence capability, so “maybe we should actually have that debate in this country sooner rather than later.”

There followed a curious exchange dealing with the difference between foreign intelligence and security intelligence collected abroad using covert means:

The Chair: Just for the record, Mr. Pratt, I don't think Mr. Elcock said that CSIS was collecting foreign intelligence. He said CSIS collected security intelligence in a foreign location.

Mr. David Pratt: Covert activity is essentially foreign intelligence, though. Would you agree, Mr. Elcock?

Mr. Ward P. Elcock: The problem with the latter part of that question is it depends on what you mean by “foreign intelligence.” If you mean by the definition of foreign intelligence that anything collected outside the country is foreign intelligence, whether it's related to threats to the security of Canada or is simply information that's important for the government to know for other reasons, then that's one case. If you think that foreign intelligence in the CSIS Act

ultimately means not all intelligence collected outside the country but intelligence that is not threat-related, which is maybe collected only inside Canada, that's complicated and it turns on all the legal language. But if you believe it's the broad definition, then there's no question that we are collecting foreign intelligence when we operate outside the country to collect threat-related intelligence.

Again, Pratt went to the heart of the issue – Did Elcock think the McDonald Commission was “off-base” or not regarding two intelligence agencies?

Elcock replied evasively: “I’m not going to comment on the policy issues,” he said, but then, being the experienced official that he is, proceeded to do just that by noting that things had changed since the days of the McDonald Commission, given that intelligence agencies such as CSIS are currently reviewed by civilian and parliamentary committees. This was true enough, but it was entirely beside the point. Pratt’s query was to whether it was time for a discussion of the desirability of creating a dedicated foreign intelligence agency. Elcock knew as well as anyone that the argument in favour of it had nothing at all to do with oversight and everything to do with specialization and the dangers of an unbalanced and unchecked single source of all national intelligence.

Later in his testimony, Elcock remarked on quite a different matter when he said Canada was not alone in having a single intelligence agency. “There are at least two or three” other countries with unified intelligence services. Elcock could, however, think of only one – the Dutch. He was silent regarding the overseas mandate of the Dutch foreign intelligence service and how it may have compared to the limited but clearly ambiguous mandate of CSIS. Nor did he offer an opinion on the effectiveness of the Dutch organization.

Other observers have noted over the years that CSIS’s contribution to Canada’s foreign human intelligence is minimal. CSIS cannot make requests to foreign agencies for specific foreign intelligence (Hensler 1995). It receives unsolicited intelligence from friendly foreign agencies, but only what these agencies choose to share with Canada, and the information may or may not be useful. Consequently, Canada’s reliance on shared intelligence is substantial. According to the Director’s Task Force of 1992, Canada’s allies provided almost all of its imagery intelligence, over 90 per cent of its signals intelligence, and much of its human intelligence (Farson 1999, 25). It is not clear whether matters have improved during the past decade. What is certainly true is that the structural vulnerabilities, present for over half a century, have not been addressed.

Pratt’s question to Elcock regarding CSIS discovering intelligence “incidentally,” or even accidentally, that affected the vital interests of Canada’s close allies, which Elcock did not answer, was discussed explicitly by Martin Rudner. According to him (as was quoted in the introduction to this report), the inability of CSIS to act “could create a gap that could have horrendous consequences” (Canada 2003a). This was one reason he thought there was a “very compelling case for a dedicated [foreign intelligence] agency.” On the other hand, Reid Morden, a former director of CSIS, has argued (Morden 2003) that the creation of a CFIS would not produce a sufficient marginal increase in intelligence to warrant the costs and risks.

In 2005, Wesley Wark reminded a special senate committee charged with studying the Anti-Terrorism Act that Canada was “an anomaly in the global community because we do not have a true foreign intelligence service” (Canada 2005b). Later in his testimony, he expanded his comments with specific reference to CSIS. It is a given, for reasons already discussed, that “a country needs a good intelligence capability that is its own: it cannot borrow from allies.” Increasingly, CSIS has acknowledged this necessity and “has increasingly begun to define itself as a dual service” that collects both security and foreign intelligence. “We may decide that that is not a bad model, but we should not have arrived there by accident or without a full review and

introspection of the process. The very fact that CSIS has moved increasingly in this direction indicates recognition of the necessity.”

About a year later, in a speech to the 2006 meeting of the Canadian Association for Security and Intelligence Studies, former MI6 chief Sir Richard Dearlove proposed that Canada establish its own foreign intelligence agency. At this same meeting, CSIS director Jim Judd stated that his organization had assisted in the evacuation of Canadian citizens from Lebanon and were part of a mission in Iraq to free a captured Canadian hostage. He also said that CSIS supported the Canadian military in Afghanistan. Kristan Kennedy remarked that these new initiatives of questionable legality and prudence were undertaken by CSIS out of “organizational self-interest” (Kennedy 2006, on-line). Wesley Wark said he thought CSIS was “jockeying for position” (Freeze 2006). Former CSIS director Reid Morden said that if a foreign intelligence capability was needed, then an expansion of the CSIS mandate would be sufficient (Morden 2006). This may have proved the point that both Kennedy and Wark are making, that CSIS was simply seeking to enlarge its bureaucratic turf. On the other hand, the option of expanding the mandate of CSIS also reintroduced the question of whether a dedicated agency, CFIS, would be preferable. This question is revisited below.

3 (c) Department of National Defence

The Communications Security Establishment captures and analyzes signals intelligence, including signals from the Taliban in Afghanistan. They are unquestionably an offensive or spy agency. The First Canadian Division Intelligence Company provides tactical and operational defence intelligence for Canadian Forces troops (Canada 2000i). First Canadian Division Intelligence Company was officially stood up and became an established unit on 27 October 1989. It is one of two permanent units of the First Canadian Division Headquarters and the only Regular Force, field-deployable intelligence unit in the Canadian Forces. It consists of two platoons: the Intelligence Collection and Analysis Center (ICAC) and the Intelligence Operations Platoon. The ICAC’s role, in garrison and in theatre, is to give the commander and staff all-source intelligence in support of operations and planning. The Intelligence Operations Platoon contains the collection assets, which includes a HUMINT section. During operations, this platoon can be joined by additional collection assets and capabilities such as counter-intelligence, interrogation, and imagery exploitation. On 1 June 2000, all these intelligence units were amalgamated to form the Canadian Forces Joint Operations Group (CFJOG) (Canada 2000c). They were stood down in December 2005 and were replaced by the Canadian Forces Joint Signal Regiment and the Canadian Forces Joint Support Group.

Whatever the theoretical, legal, and bureaucratic issues between security and foreign intelligence, military intelligence is simply a requirement of effective operations. As a consequence, more than national pride and a sense of grand strategic purpose are involved: lives may be saved or lost as a result of operational effectiveness. In describing the structure of military intelligence in Canada, we also consider the evidence of recent operations prior to Afghanistan.

Combat intelligence in small operations is typically collected by soldiers in three phases: (1) top-down guidance and direction for HUMINT gathering efforts; (2) the actual collection of intelligence – through reconnaissance operations, for example; and (3) the analysis of information at brigade level (Watson 2001). The collated intelligence product then moves in two directions. Strategic intelligence is sent to division and headquarters level where it is assessed in the J2 Intelligence Directorate and relevant information is provided to political leaders, while tactical intelligence is disseminated down to battalion and company level for use by front line soldiers.

This is more or less standard procedure for modern military forces. Intelligence support for peacekeeping and, *a fortiori*, peacemaking operations, however, presents a new set of problems. Nowhere is Canada's lack of a foreign intelligence capability more obvious than in its impact on multinational peacekeeping, peacemaking, or stabilization operations. Since these activities, whatever they may be called, are not likely to diminish as long as Canada retains even the most modest military capability and because these activities are real military operations, it may be useful to consider this issue in some detail.

Since 1956, international peacekeeping has been a basic tool of Canadian foreign policy and has some degree of international influence – though the actual degree of influence is contested. Intelligence support for multinational or coalition operations has been one of the most pressing problems for the Canadian government and for the Canadian Forces in the last decade and a half. Information operations within the United Nations, which are never simple or easy, present additional difficulties that are made worse by the shortcomings of the intelligence community in Canada, and of course, in the United Nations.

The lack of nationally collected foreign intelligence in Canada has compelled the Canadian Forces to depend on its allies in peace support operations. Because Canada's intelligence community was designed in some measure to meet the needs of its allies rather than to focus on its own needs, and even more importantly, because Canadian intelligence production does not, in fact, do much to meet the needs of its coalition partners, *on intelligence grounds alone*, the worthiness of Canada as an ally has become questionable to Canada's traditional partners.

Consider, for example, the assessment of General Sir David Ramsbotham in his *Peace Enforcement: Organizational Planning and Technical Requirements* which identified six distinct intelligence requirements for peace support operations, all of which Canada should be able to provide not only for itself, but in order to assist the coalition or multinational force to which Canadian Forces on peacekeeping operations have typically been assigned (Ramsbotham 1995). All of these remarks with respect to peacekeeping apply even more emphatically to more robust military operations. The first is strategic intelligence, which provides an assessment of the milieu in which Canadian troops have been deployed. Second is political intelligence, which determines the nature and intention of the leadership of the target country. Third, economic and social intelligence identify socio-economic concerns that might affect the deployment. Fourth, operational intelligence is used to plan the deployment of resources and to carry out the United Nations mandate, particularly in fluid and politically turbulent situations. Fifth, tactical intelligence for troops on the ground is required to monitor cease-fires in border areas and to alert personnel to potential dangers. The sixth requirement is counter-intelligence/counter-espionage, which aims to pre-empt intelligence operations by hostiles. These requirements are critical to any peacekeeping activity as well as to any deployment that is part of a war-fighting coalition such as the NATO mission in Afghanistan. None of these requirements can be met because, CSE aside, Canada lacks a foreign intelligence capability. The practical, political, real-world implications are significant.

Intelligence support has always been essential to the effective execution of a military mission. Without such support, Canada can only participate as a dependent junior partner in a coalition deployment. Unless a commander, even a United Nations commander, has accurate and timely information about the armed groups he is separating in a classical peacekeeping operation, he cannot position his forces in the most effective manner. He must also have access to current information on political changes that will shape future military action. He must know leaders on all sides and study their tactical methods, personalities, and motivations (Elliot 1981, 557).

Prior to deploying Canadian troops on Operations Other Than War, the Canadian Forces Strategic Reconnaissance Group (SRG) undertakes a detailed risk assessment to determine if Canadian

troops face an unacceptable risk in any area of responsibility. Estimating risks requires an intimate grasp of the culture and capabilities, the politics and psychology, of hostiles and of potential hostiles (Handel 1989). Intelligence analysts prepare this assessment based on raw data. Canada, however, having grown accustomed to receiving a finished intelligence product from its allies, has allowed its analytic capability to atrophy. Hence, it must create Canadian threat assessments based, for example, on American data, relying on external sources that may not have Canada's interests in mind or have Canadian expertise with respect to the actual problem at hand and of concern to the Canadian government. Moreover, the deployment of an SRG to a target country a week before the arrival of the main force does not provide enough time to prepare a full intelligence picture for force commanders. Canadian intelligence simply cannot provide such a picture by itself. This is important to Canadians whether they think the Canadian Forces are chiefly a peacekeeping formation or a war-fighting one because it implies that Canadian soldiers will be sent into a threatening environment with a picture of what they are getting into that is less clear and less complete than it otherwise might be. That is, the lack of a Canadian intelligence capability increases the danger for Canadian troops.

Nor can Canada rely on the United Nations for intelligence support (Dorn 1999). The United Nations cannot undertake information gathering or espionage operations and still maintain its impartiality. United Nations doctrine holds that military intelligence collection is incompatible with peacekeeping because such collection can undermine two fundamental conditions for peacekeeping: the impartiality of United Nations forces and the support given to United Nations forces by the belligerents (Elliot 1981). United Nations information resources and analytical capabilities are, in any event, simply inadequate. For example, Major General Trond Furuhovde, former commander of United Nations forces in Lebanon, reported on United Nations intelligence support in the following terms:

The information element is often very vaguely defined and consequently vaguely executed. The importance of exact and timely information flow must again be underlined. In several instances information collection and intelligence analysis were reduced to nearly useless activities. Exact and timely information is essential to safeguarding your troops and knowing the actions taken by the belligerent. (Furuhovde 1995, 24)

The implications of poor or non-existent intelligence have been documented on several occasions. In principle, deploying Canadian troops without proper intelligence as peacekeepers, in peace-support operations, or as combat infantry is bound to result in sub-optimal effectiveness and reduced influence.

United Nations missions to the former Yugoslavia, where Canadian troops had a vanguard role, and to Rwanda and Zaïre/Congo, where Canada had a "leading nation" role, provide recent examples of these problems. The "leading nation" is also assumed to be the leading *intelligence* nation (Smith 1994, 178). Unfortunately, the limits to Canada's HUMINT assets and to its analytical capabilities prevented it from collecting and synthesizing intelligence in a timely manner. These shortcomings, combined with the inability of the United Nations to provide intelligence support, made Canadian participation in United Nations operations difficult and much more dangerous than they need to have been (Keeley 2004). A brief survey of three peacekeeping operations outlines this as clearly as possible.

3 (c) i. *Yugoslavia*

During the 1990s, the “key peacekeeping operations” for the Canadian Forces were in the former Yugoslavia, including Kosovo (Granatstein 2002, 399). The military difficulties encountered by the Canadian Forces at Sarajevo, Medak, and Srebrenica, as well as the atrocities committed by Serb and Croatian forces, are perhaps the best known aspects of this conflict; the Canadian mission to the former Yugoslavia also faced failures of military and civilian intelligence. The Canadian Forces publication *Dispatches* described the intelligence problems encountered in the former Yugoslavia:

With minor exceptions, United Nations-generated intelligence support was virtually non-existent and of no use to units. Canadian-based intelligence collection resources, including imagery exploitation, were incapable of responding quickly enough to provide timely support to units in-theatre. (Canada 2001g)

The Canadian Forces have only recently acknowledged that human intelligence is essential to intelligence collection for peace support operations: “HUMINT, gathered by well-trained troops in an area of operations, from interacting with the complete range of local human sources, provides ... critical information from which a complete intelligence picture can be developed” (Canada 2001g). *Dispatches* stated in 1996 that the British and French forces in Bosnia obtained 98 per cent of their information from HUMINT sources, primarily soldiers on patrol (Canada 1996b). This option was not available in Sarajevo to Major General Lewis MacKenzie in 1993, who had neither the mandate to conduct reconnaissance nor the intelligence staff to analyze such information:

Peacekeeping in a theatre such as UNPROFOR [United Nations Protection Force in Former Yugoslavia], where the opposing forces are constantly maneuvering, demands an intelligence function. There have been several instances where an advance knowledge of the probable intentions would have been extremely helpful, such as the Croatian offensive of January 1993, yet the lack of authority to conduct a proactive intelligence function makes this extremely difficult to do. (Johnson 1997, 204)

In order to gather intelligence, which was essential but unavailable through United Nations, Canadian, or American sources, Major General MacKenzie and other Canadian commanders authorized clandestine reconnaissance patrols – black ops – to obtain the information needed by Canadian soldiers (Naime and Owen 1993). These covert missions placed Canadian troops at great risk, but they had no other means of collecting much-needed but otherwise unavailable information. Again, reliance on external intelligence sources backfired for Canada. Unless Canada can develop a unilateral ability to obtain information, its role in any multinational deployment, particularly in a vanguard role, will likely meet with failure as well.

3 (c) ii. *Somalia*

For Canada, the United States, and the United Nations, the Somalia mission that began in 1993 was confused, not to say hopeless. Certainly, it was also characterized by weak Canadian intelligence. This operation demonstrated the need for a full range of civilian and military intelligence to assess the potential threats to the troops in theater. The 1997 *Report of the Somalia Commission of Inquiry* made an obvious generalization regarding intelligence support for United Nations Task Force Somalia: “countries that do not have their own intelligence support, typically for conventional military operations, do not have appropriate procedures for collecting, processing, and disseminating information for peace support operations” (Canada 1997c). This

also had a specific application, because Canadian troops on the ground had no intelligence from Canadian sources and had to rely on other sources, especially the United States.

During Operation Deliverance, Colonel J. S. Labbé, Commander of the Canadian Joint Forces in Somalia, believed he could rely on the United States, which was in operational command of the mission, and he had agreed unofficially to share intelligence. Weeks later, Labbé expressed dissatisfaction with this intelligence support, describing it as uneven and fragmentary, but it was all he had (Canada 1997b). Without a way to gather independent information and lacking intelligence from American, Canadian, or United Nations sources, the major formation, the Canadian Airborne Regiment, had to rely on media reports, particularly from CNN.

Once in-theatre, Labbé realized American intelligence was not always reliable, and he had trouble obtaining information in a timely and responsive manner. The junior leaders and soldiers had little information about what to expect on arrival and almost no operational or tactical intelligence to guide them other than what was collected on patrol. Poor intelligence was one of several problems with the deployment; Others were difficulties with mission statements, rules of engagement, and disciplinary issues within the Airborne Regiment. Intelligence shortcomings exacerbated these problems, and as David Bercuson noted, “the mission the Airborne ultimately embarked on was very different from the one it had prepared for” (Bercuson 1996, 228). The Canadian mission to Somalia included a failure of intelligence on a mission where Canada did not take a “leading nation” role, offering yet another instance of the lesson that Canadian foreign intelligence assets are necessary to support a Canadian contingent as well as to support the coalition intelligence effort. If Canada had access to better independent foreign intelligence about the factional leaders and hostile environment, the Airborne Regiment might have been better prepared; indeed, Canada might have refused the Somalia deployment entirely. If Canada aspires to deploy in an “Early In, Early Out” (EIEO) role, as espoused by former Minister of National Defence Art Eggleton, preventing intelligence errors such as those experienced in Somalia are a simple and obvious condition of accepting an EIEO mission. This can only be done through an expanded and independent foreign intelligence capability.

3 (c) *iii. Rwanda*

In 1994, Canadian Major General Romeo Dallaire was selected to command the United Nations Assistance Mission to Rwanda (UNAMIR). From the beginning, he was plagued by the United Nations bureaucracy and by a general lack of information, let alone insightful intelligence, of the theatre of operations. Thus “with a confidence born of ignorance, we soldiered on” (Dallaire 2004, 47). There simply was no intelligence to be had from Canada or from anywhere else; there were no military maps so they used tourist materials to plan military operations. Non-government organizations and journalists passed on information, but it was impossible to assess. United Nations headquarters in New York provided little information (Off 2000). Worse, the Rwandan ambassador to the United Nations had a seat on the Security Council, thus he was privy to all the intelligence that came to that body. In contrast, wrote Dallaire, “there I was with my small team of intelligence officers who were risking their lives for crumbs of information while the extremists had a direct pipeline to the kind of strategic intelligence that allowed them to shadow my every move” (Dallaire 2004, 195). Also, the Permanent Five powers of the Security Council, with their own agendas, did not provide policy-neutral inputs or advice (Quiggin 1998). Without intelligence from others and incapable of producing his own, Dallaire was blind. The consequence has quite properly been described as genocide.

In retrospect, after the damage was done, other flaws in the Canadian intelligence process came to light. In the analysis by the Army Lessons Learned Center of Operation Assurance to Rwanda, a lack of coordination between DND, DFAIT, CIDA, and other agencies was noted. There was no national strategic concept for intelligence operations, nor any direction about intelligence collection, coordination, and responsibilities. Neither United Nations nor Canadian intelligence sources provided prior intelligence on the situation. The intelligence support that was available was proffered in piecemeal fashion because a lack of intelligence architecture within the federal government made the passage of critical information subject to lengthy delay (Canada 1997b). In short, Canada's inability to collect foreign intelligence in support of UNAMIR crippled the Rwanda deployment, contributing both to the tragedy on the ground and to a foreign policy debacle for Canada; it also put all the United Nations troops at great risk. As Carol Off pointed out, the non-permanent Security Council members, such as Canada have:

[no] veto and, as lesser powers, they haven't got the same intelligence-gathering abilities as the big players, who knew all too well what was going on in Rwanda (the CIA had reported to its masters the possibility of mass killings as far back as January). The Permanent Five didn't share their knowledge, however, and Boutros-Boutros Ghali wasn't passing on the dire messages that his DPKO [Department of Peacekeeping Operations] had been getting from Rwanda for months. (Off 2000, 70)

The emotional response to genocide, which is understandable enough, need not obscure the obvious point with which we began this discussion: states have interests, and for whatever reason, states with reliable intelligence concerning Rwanda were not willing to share it; nor was the United Nations.

3 (c) iv. *Zaire*

The sequel to Rwanda, Operation Assurance, took place over the winter of 1996–97 (or rather, it failed to take place). Following the Rwanda genocide, the losing Hutus fled west to Zaire; some were civilian refugees and some were armed militias and remnants of the Hutu Rwandan army. They displaced Zairian Tutsis, some of whom fled east to Rwanda, some of whom began killing the migrating Hutus in an alliance with Laurent Kabila, a tribal war lord rebelling against the Zairian government. The Zairian government, in turn, declared eastern Zaire a war zone and began military operations. The United Nations then dispatched Raymond Chrétien to the region. He had been there about a week, mostly flying among capital cities talking with officials, when he had a phone conversation with his uncle, the prime minister.

It was clear from discussions at United Nations headquarters that neither France nor the United States would take a leading role. Jean Chrétien then said that Canada would do the job and sent Lieutenant-general Maurice Baril to the area with an advance party. The deployment of this small force was rapidly overtaken by events: increased fighting in Zaire sent refugees back into Rwanda, and by the end of the year, the Canadian contingent had also left. This eight-week fiasco was extensively studied by the Canadian Forces and resulted in a lengthy "lessons learned" exercise (Hennessy 2001; Cooper 2002; Kasurak 2003; Canada 2007). Most of this analysis dealt with command and control and readiness planning, and it proved useful when Canadian troops were sent to Afghanistan. On the intelligence side, however, the lessons are still being learned.

As the recent document, *Leadership in the Canadian Forces*, noted: "Canada lacked the necessary intelligence-gathering capabilities and there were no mechanisms in place to effectively

share available information located in several government departments and agencies in Ottawa” (Canada 2007, 17). More specifically, the force commander, General Baril, could never determine how many refugees there were, nor where they were located. As he reported to a SCNDVA hearing in 1998, “we don’t have our own national sensor to be able to know what is going on in the heart of Africa. We don’t have such means. We have to rely on our allies” (quoted in Kasurak 2003). The allies, in this instance the United States and the United Kingdom, relied on aerial reconnaissance and satellites. This meant that only refugees who could be seen from the air – and the American Orions and British Canberras were forced to fly at high altitudes because of ground fire – were counted in the official tallies. The number of refugees in the bush remained unknown. The conclusion is obvious: “Operation Assurance was a thorough-going intelligence failure” (Kasurak 2003). That is no doubt one reason why it was known to the troops as “the bungle in the jungle,” and why no record of it appears on the DND “Past Operations” website.

The larger conclusion to be drawn from participation in United Nations missions, whether in a leading nation role or as a member of a multinational deployment, is that Canada cannot rely on its allies to provide HUMINT. A finished intelligence product from the United States (or conceivably, the United Nations) is frequently missing when it is most needed. Canada’s poor intelligence support capabilities affect its interaction with its allies and add to Canada’s intelligence dependence on its allies. These experiences also suggest that Canada must refrain from engaging in future peace support operations without a clear strategic concept, a mission statement for Canadian troops, and adequate intelligence support. The need to rely on foreign intelligence results not simply in the symbolic degrading of Canadian sovereignty; it is dangerous to Canadian troops, reduces the level of autonomy for Canadian political and military leaders, and compromises entire missions. Because Canada’s foreign intelligence assets are so limited, they cripple Canada’s foreign and defence policies, especially United Nations-mandated peacekeeping operations that historically have carried so much symbolic weight for Canadian policy-makers and the Canadian public.

3 (d) Other Government Units

DFAIT had a Foreign Intelligence Bureau until 1993, when the entire unit was transferred to the Privy Council Office and became the Intelligence Assessment Secretariat; then, in 2004, it became a contributor to the Integrated Threat Assessment Centre (ITAC), the purpose of which is to provide comprehensive threat assessments to the intelligence community as well as to first responders such as the police. Secondly, ITAC liaises with similar organizations in the United States, the United Kingdom, Australia, and New Zealand. The ostensible purpose of these changes is to streamline Canadian intelligence assessment, to increase the cohesion and co-operation of the intelligence community, and to redefine the marketing of the intelligence product (Farson 1993, 56). It is not clear whether this purpose was achieved. Only a small portion of the original DFAIT assets and resources survived the 1993 transfer (Wark 2001). DFAIT still retains a Security and Intelligence Bureau that supports policy and operational decisions and advises the minister on intelligence activities (Canada 2002c). Although the exact size and composition of the Bureau is classified, it represents DFAIT’s interest in, and need for, foreign intelligence and provides some expertise on specific international issues relevant to Canadian foreign policy.

The Bureau is responsible for providing timely and critical intelligence on world events, assuring the protection of Canadian personnel and their families, safeguarding government premises and assets, promoting and protecting Canadian national interests and all NATO classified matter conveyed to Canada, and maintaining communication security. The Current Intelligence Division of the Bureau produces briefs for senior managers and analytical, operationally relevant

assessments and updates on breaking events. The Foreign Intelligence Division provides information support for department operations and ensures the coordination of intelligence activities. The security divisions are responsible for security and personal safety at DFAIT headquarters and abroad, including the security of buildings, information and information technology, personnel security, clearances, investigations, and security education. None of this activity, which is essential to departmental operations, involves spying. Moreover, the 1993 transfer of foreign intelligence assessment from DFAIT to the PCO further reduced an already low level of expertise in the area of intelligence analysis (Farson 1999). In 2000, a forty-five-page audit of security in DFAIT was silent concerning any intelligence function for the department (Canada 2000b). The current role of DFAIT in foreign intelligence seems to have been reduced to collection through open sources by officials posted abroad. Such a rudimentary collection and analysis is clearly not sufficient to support Canada's extensive international relations nor, given the "soft power" approach to international politics developed by DFAIT for much of the past decade and a half, does one have confidence that the department has a serious mandate to defend Canadian interests, as distinct from an elevated, soft-power reputation cherished by senior DFAIT managers. These considerations make it imperative for DFAIT to change its traditional ethos before it would be a suitable home for any CFIS.

The only other government organ with a direct interest in intelligence is the Privy Council Office. This is because the prime minister has ultimate responsibility for Canadian national security (Canada 2001f). One task of the clerk of the Privy Council, Canada's highest-ranking public servant (in effect, the prime minister's deputy minister), secretary to the cabinet, and head of the public service, is to chair the most senior committee dealing with intelligence and to oversee a number of secretariats dealing with intelligence assessment and analysis. It is a chain-of-command organization that may well be the critical junction within the Canadian intelligence community. Within the Privy Council Office, the national security advisor to the prime minister is supported by two secretariats, an International Assessment Staff, which deals with trends in foreign affairs, and the more important Security and Intelligence Secretariat, which supplies substantive advice on national security to government and manages border relations with the United States. However, the committee organization and traditional bureaucratic ethos of this public service office are likely to impede, rather than enhance, the effective analysis and collation of intelligence. The transformation of an imaginative intelligence analysis organization into a bureaucratic routine is a common problem with intelligence organizations around the world (Codevilla 1992). There is no reason to think that the Privy Council Office is an exception.

4. PROBLEMS

The sketch of the structure of the current Canadian intelligence community provided in the previous section, particularly with regard to military intelligence, has already indicated a number of obvious problems. This section delineates some underlying reasons for them while the following sections outline what would be an appropriate response.

The fundamental problem is historical and institutional: The tendency to rely on allied foreign intelligence combined with the reluctance to expand Canada's foreign intelligence community are responsible for Canada's current intelligence shortcomings. As noted, Canada is one of the few countries in the world without a service dedicated to the collection of foreign intelligence abroad by human means, and the only G8 country without this capacity. Unlike its principal intelligence partners, the United Kingdom and the United States, intelligence has never been imbedded in Canada's political culture. Canada has never been a principal military or economic power with vast overseas interests. Instead, historically, it has gathered intelligence to meet the needs of its senior coalition partners. Canada has never had a foreign intelligence service or involved itself in covert operations except during wartime, the memory of which has been nearly expunged from the nation's collective and institutional memory. It is too early to determine the consequences for intelligence-gathering, especially for HUMINT, from the on-going Afghanistan deployment.

4 (a) No Interest in Foreign Intelligence

The most obvious reason why foreign intelligence has received little public attention in Canada is because officials have kept the matter quiet, thus Canadians have shown no interest in the matter. Most Canadians therefore have little understanding of the role of intelligence in either domestic or foreign politics. More surprising, however, is that, at least after Sir John A. Macdonald's time, government leaders have also shown little interest. For example, Anthony Campbell, the former executive director of the Intelligence Assessment Secretariat of the Privy Council Office, stated at the 2001 CASIS conference that the Canadian government must reform how it uses intelligence and make a concerted effort better to understand the intelligence process and how it is to be used. The government (by which he meant both politicians and bureaucrats), Campbell asserted, strongly resists any changes to intelligence methods and to the allocation of funds (Campbell 2001).

There are two other reasons why there has been no serious debate about foreign intelligence in government circles. If information about Canadian foreign espionage activities became public, it could prove embarrassing to the government and might jeopardize Canada's diplomatic relations. Secondly, using human agents undercover for intelligence collection can be dangerous. From the days of Norman Robertson, DFAIT has been risk-averse with respect to anything having to do with security (Granatstein 1981, 330). Starnes reported, for example, that when he was ambassador to the United Arab Republic, he ordered the Canadian embassy to keep some CIA encryption rotors during the Suez crisis so they would not fall into Soviet hands if an Egyptian mob stormed the American embassy. Some "nervous Nellie" in External in Ottawa "thought that Canada's fragile virginity might be compromised in some way by my decision" (Starnes 1998, 119). In short, timidity and the anxieties that accompany risk-taking combine to explain why many government officials prefer to avoid the issue of spying altogether.

Starnes himself, who said he had no principled opposition to spying, also opposed the creation of "Espionage Canada" on the grounds, he said, of "realism," of "hard-headedness," and of practicality. "I do not know," he said, "whether the information we are receiving from our present intelligence-gathering activities is adequate for our needs" (Starnes 1998, 155). However, as

noted above, without an independent source of foreign intelligence, it is logically impossible to determine whether foreign intelligence shared by Canada's allies is "adequate for our needs." There is simply no way to know.

Secondly, Starnes said that he had not "seen or heard convincing arguments of a present and urgent need for an espionage service. Certainly the argument that we should have one simply because other countries have one is not very convincing, and I have reservations about our ability to operate and control such an unusual asset" (Starnes 1998, 156). In fact, what is "unusual" is *not* having a foreign intelligence capability. Moreover, no one has made the argument that because other countries have spies, Canada should have them, too, as if a spy service were akin to a flag or an anthem. Rather, they give reasons for creating a foreign intelligence service, reasons that can be analyzed and discussed. Starnes, an Anglo-Quebecker, did allow that a hostile and independent Quebec might be sufficient grounds for an espionage agency – but that possibility is increasingly remote.

In response to the institutionalized opposition from diplomats and officials in foreign affairs, one might say that in principle, their business involves deception and intrigue so that the option of refusing to engage in espionage and foreign intelligence-gathering necessarily reduces the ability of the country to defend its interests. Stuart Farson sums up why this debate over establishing CFIS lost momentum in the past: timidity, lack of official interest, and bureaucratic turf-protection aside, apart from the FLQ crisis, terrorism (including the bombing of Air India Flight 182 in June 1985) has historically been sporadic or directed offshore. Terrorists in Canada have been careful not to open insurgency operations on a scale even remotely like that suffered by the United Kingdom in Northern Ireland. In part, this has been a rational response so as not to attract attention to themselves in order quietly to go about the business of fundraising and staging for attacks on targets outside Canada, including America (Harvey 2004; Bell 2004; Thompson and Turlej 2003). Looking further into the past, geography has isolated Canada from most foreign threats: large oceans (one impassable most of the year) and a large, friendly neighbour have meant that Canadian intelligence needs have consisted chiefly in early warning systems operated with the United States and a security intelligence network largely kept in reserve (Farson 1999).

Unfortunately, new and unanticipated threats emerged after the end of the Cold War for which these minimal intelligence functions are inadequate. The terrorist attack on 9/11 and the oft-stated determination by the government of Canada to play a significant role in international affairs, whether inside the United Nations or as a member of some future "coalition of the willing," requires and implies a capability to produce accurate and timely intelligence. Even so, the government continues to assert that these requirements can be met because Canada obtains adequate foreign intelligence from its sharing agreements. As we have seen, however, dependence on the American intelligence community unnecessarily limits Canadian sovereignty and restricts Canada's ability to deploy its resources, including troops, in an effective manner.

4 (b) Intelligence Dependence

A few of the inherent problems that intelligence dependency imparts to the coherent development of foreign and defence policy have been discussed in passing; In this section, they are made explicit, beginning from the position that, in principle, states seek to retain an ability to monitor covert foreign influence in their territory. Accordingly, a permanent security intelligence capability is needed, not just in times of war, but also in peacetime or for peace-support operations or operations other than war (Hermann 1996). Complete dependence on others reduces not only the strategic options available to a country, but its sovereignty as well. As we have seen,

owing to Canada's heavy dependence on the American intelligence community, Canadian access to information relevant to Canadian policy interests has been impaired. In the interest of maintaining secrecy, the United States distributes information throughout the Western intelligence community based on the "need to know" rule.

This is based on the assumption that if information is restricted to people who need to know it to carry out their tasks, it is less likely to find its way into unauthorized hands. Because of their more limited interests abroad, the smaller partners in the community [such as Canada] are generally deemed to have a smaller requirement for information than does the United States. (Hermann 1996, 91)

This principle applies even for such relatively innocuous intelligence sharing such as that between Canada and Australia. In the early 1950s, for example, the British Commonwealth established a defence intelligence exchange program administered in Canada by the Joint Intelligence Committee. The Australians agreed to share intelligence with Canada "subject to oversight by the [Australian] Defence Committee," but "it suggested that the provision for the Defence Committee to oversee material transmitted ... would not need to be brought to the attention of the Canadians, as it would be a domestic matter" (Australia 1954). In other words, the Australians, like the Americans, were perfectly willing to share intelligence on some things selected by them. Canada, no doubt, would reciprocate.

In general, as Robert Kaplan has argued, "to expect human beings and organizations to think about the interests of others before their own is to ask them to deny their own instincts for self-preservation" (2002, 42). Indeed, the same organizational imperative applies as strongly to charities and international NGOs as it does to the Australian Department of External Affairs. Relief charities, Kaplan points out, "lobby for intervention in areas where they are active, rather than in areas where they are less so." Thus, he argued, the media gave more attention to Bosnia than to South Ossetia not because one area was more violent or filled with atrocities than the other, but because more relief charities were at work in the Balkans than the Caucasus (Kaplan 2002, 44).

Therefore, there necessarily exists constant tension among the interests of the receiving country, of the alliance, and of its dominant partner. As Martin Ruder said in his testimony before the Standing Committee on National Defence and Veterans Affairs (SCONDVA) in 2003:

Just briefly, in very informal conversation with our allies, it's interesting to note that our allies like the status quo for a variety of reasons, both selfish and unselfish. The selfish reason, by the way, is that they know Canada is a net importer of foreign intelligence. Whose foreign intelligence are we importing? Theirs.

They don't necessarily control Canada's agenda. They can't. But they certainly control a large part of the information available to Canada that is used to determine our agenda. I'm not saying they're malevolent, but they know pretty much what the Government of Canada knows. (Canada 2003a)

Whether foreign producers of intelligence derive an immediate benefit or not by importing a finished intelligence product from Australia in the 1950s or from the United States or Britain today, Canada is buying a foreign perspective on secret or stolen information, which means that the flow of finished intelligence to Canada is not determined by its own interests (Whitaker 1991). The value of such information is always difficult (and sometimes impossible) to judge because of silent oversight and need-to-know restrictions – one never really knows what is left out, distorted, or delayed. Information provided by the United States, for example, suits what

American intelligence sources want Canada to know, or what they think Canada should know. Accordingly, Canadian security policy is being made on the basis of American information, which in turn, may have been shared in order to promote American interests. Even with the best will between the two countries and with full disclosure, Canada would still suffer from American mistakes or weaknesses. There are several reasons why this is not in Canada's national interests.

First, American perceptions of Canadian intelligence requirements are not always accurate or appropriate to Canada's political and military situation. Moreover, the Government of Canada knows it, not simply because they have had to deal with the results of dependency in botched peacekeeping operations. As long as the 1986 *SIRC Annual Report*, for example, the statement was explicitly made that relying on friendly foreign intelligence services did not allow the recasting of information in Canadian policy terms (Canada 1987). American-supplied intelligence must always have an American focus because it is designed for American consumers. Again, American information reaching Canada will always be censored to prevent information that the United States considers sensitive from reaching non-American recipients, if only to maintain operational security over sources and methods (Ramsbotham 1995, 76). This is true not only for Canada but for any UKUSA partner (Richelson and Ball 1990). Of course, Canada also has intelligence meant for "Canadian Eyes Only."

With respect to Canada, there may also be reasons related to American national interests that would prompt the United States to withhold intelligence. Because of the secrecy of such non-events, examples are inherently difficult to track and not likely to be publicized. Press reports indicate that Canadian SIGINT overheard the American ambassador "discussing a pending trade deal with China on a mobile telephone and used that information to undercut the Americans in landing a \$2.5 billion Chinese grain sale" (Goodspeed 2000, online). Likewise, Jane Shorten, a former CSE employee, suggested that Canada mounted operations against both the United States and Mexico in 1993 because Canada suspected that its American partners were withholding trade-related information prior to the conclusion of the NAFTA agreements (Livesey 1998). Alistair Hensler also argued that American intelligence was active against Canada: "during negotiations on setting up the North American Free Trade Agreement" (1999, online). Some Ottawa bureaucrats, however, "thought that we shouldn't spy on Americans, [because] it was unethical, but the Americans were spying on us" (Sevunts 2000, online). David Frost and Michael Gratton (1994) stated categorically in *Spy World* that the United States routinely engaged in SIGINT operations against Canada. Former CSIS director Reid Morden in 2001 also suggested that American intelligence has not always honoured the friend-on-friend principle that prohibits targeting Canada in anything but a joint operation (Brown 2001). The logic of commercial intelligence gathering even in the context of friend-on-friend prohibitions is clear enough: even allies are competitors.

These allegations are anecdotal and do not constitute evidence that might prove useful either in a court of law or in the court of public opinion. As far as intelligence is concerned, however, courts of competent jurisdiction do not exist. What counts, at least in common sense terms, is that the sources of the anecdotes are credible and that they are consistent with the general assumption made, that is, that intelligence is acquired routinely as part of the promotion of a nation's interest. It is simply a fact that Canada relies on intelligence from a foreign country that, however friendly, has conflicting or competitive interests and routinely withholds or alters information. As a result, American-source intelligence has been inaccurate and untimely, and in the future it may well be deceptive or intended to give the United States a competitive economic advantage. Even without a deliberate attempt to disinform Canada, and assuming the Americans share intelligence they believe is correct, without an independent collection or analysis capability, Canada is forced to accept the American intelligence at face value, which may effectively obliterate any significant

difference between, and informed discussion of, Canadian and American foreign and defence policies. Despite their cost-effectiveness, current intelligence-sharing agreements with the United States are not the ideal way for Canada to obtain foreign intelligence.

This dependence will probably increase in the next decade. In late 2001, the Federal Bureau of Investigation asked the American Congress for more money to increase its permanent presence in Canada, in order both to prevent terrorist attacks on the United States and to deter cross-border crime. The implicit message was that Canada could not adequately provide intelligence gathered within its borders to its southern neighbour, and that the Americans must do it for themselves (Daly 2001). We have already seen that American intelligence does not often meet Canadian intelligence requirements. Now, however, the United States has publicly declared that it is prepared to collect intelligence in Canada on its own, which is a clear indication that Canada has little to offer them in return.

This already unhealthy dependence on the United States is likely to become worse should the Americans, with a heightened concern with security post-9/11, decide to restrict further the flow of intelligence to Canada. American national security advisor Richard Perle summed up the new American attitude towards intelligence coalitions: “one hopes that won’t be necessary – but I can promise you that if we have to choose between protecting ourselves against terrorism or a long list of friends and allies, we will protect ourselves against terrorism” (BBC 2002). With the new priority on ensuring its own intelligence requirements, the United States may well become more unilateralist and less interested in passing intelligence to Canada. Deprived of American intelligence, Canada will be blind; it will also lack the ability to gather foreign human intelligence for itself. Such a condition obviously increases Canadian vulnerability. This would seem to be even more the case when the foreign affairs culture has been systematically deprived of its own foreign intelligence over a long period of time. Thus, looked at simply in terms of ensuring the continuation of Canadian access to (and dependence on) United States-source intelligence, and independent of whether it is in Canadian interests to meet its own requirements in this area, it is unquestionably in the national interest of Canada to develop a foreign HUMINT capacity in order to retain its worthiness as an American ally.

4 (c) The Downside of Intelligence Sharing

In 1998, Alistair Hensler noted that intelligence sharing agreements involving Canada might become less effective in the post-Cold War era. The countries involved in such sharing agreements were likely to develop increasingly diverse and more nation-specific priorities of their own, he argued, and Canada’s allies would likely be collecting intelligence about threats such as terrorist groups and other non-state entities. Accordingly, they would be more likely to wish for alliance partners capable of producing raw intelligence that the recipient partner could then analyze for its own purposes. That is, the end of the bipolar simplicity of the Cold War, when differences between alliance members were small (at least with respect to confronting the USSR), means that national security and intelligence agencies, including Canadian ones, will increasingly look to their own national interests in a multipolar world. It also means that if Canada wants to maintain the quid pro quo of alliance memberships and also meet its own needs, it will have to develop broader capacities for foreign intelligence.

In particular, Canada’s primary value in the UKUSA Agreement was its geographical position vis-à-vis the former USSR. That advantage lessened as the importance of Soviet and then Russian signals declined and as satellite intercept systems were developed to monitor SIGINT targets that previously could only be covered from Canada (Farson, 1993). The gap between the intelligence

contribution Canada makes to the coalition has increased compared to what it receives. Finally, Canada's reliance on the CSE and other technical means of foreign intelligence collection may well prove less important with the rising costs of interception and cryptanalysis.

The CSE has been Canada's primary collector of foreign intelligence and the mainstay of its contributions to allied intelligence coalitions. As have other Western intelligence agencies, Canada has relied too much on technological means of collection. The American intelligence community remains heavily reliant on antiseptically clean and very expensive technically gathered intelligence. Historically, the chief reason for reliance on technological means of war-fighting, including intelligence, is force protection. Because suffering casualties causes more political problems than ever before, using technology to monitor emergent situations instead of risking human lives suits democratic political leaders during periods when democratic citizens are relatively unwilling to accept casualties. During the Cold War, technologically acquired intelligence was the best source of strategic intelligence, and it retains its importance today. It is equally important, however, to know the limitations of intelligence gathered in this fashion.

4 (d) SIGINT – Putting All of Canada's Intelligence Eggs in One Basket?

During the Cold War, Canadian and American SIGINT assets such as the Lacrosse satellite, the ECHELON system, and the Canadian Cray supercomputer targeted the USSR and its Warsaw Pact allies in order to determine Soviet Bloc capabilities and intentions. There were many challenges, of course, to the success of the operation, but the opposition was at least a clear and distinct, hierarchically organized target. By comparison, current non-state military threats are amorphous and transnational, and their non-conventional networked structure and methods make conventional identification extremely difficult (Cooper 2004b, chap. 5). It has been argued, for example, that the failure of American intelligence prior to the terrorist attacks of 9/11 was a result of having successfully built an intelligence community that was a mirror of the now-defeated enemy – in this case, KGB and the Soviet Union. The assumptions were accurate enough for 1945 and helped win the Cold War, but they are not appropriate to countering terrorists. Those assumptions regarding the purpose of KGB, which necessarily inform Canadian technical operations as well, may be summarized as follows:

1. The chief task of KGB was to penetrate the Western opposition and transmit secrets to a central authority that then would conduct analysis and plan operations. KGB's chief concern was to learn what Western services knew, and the best way to do that was to plant agents inside them;
2. Use Western moles to obscure Soviet activities, intentions, and capabilities;
3. Steal technical intelligence on, for example, A-bomb development;
4. Control or influence Third World leaders.

Western intelligence was designed to counter these purposes; to do so, a mirror organization – a “looking glass”, to use the title of John Le Carré's famous spy thriller – was built. Increasingly the United States grew dependent on technical means of intelligence-gathering and emphasized intercepting Soviet communications. The Soviets relied more on recruiting agents inside Western organizations of power.

During the 1970s and 1980s, Western intelligence tended to look on terrorist organizations as entities guided by KGB rather than as independent actors. To a certain point, this was not entirely

misguided, though they were not satellites akin to the East European secret police. By the time of the first Gulf War, the Soviets were gone, but the Western intelligence agencies did not know how to understand the new hostile organizations such as al-Qa'ida. To make matters even more opaque, al-Qa'ida looked very much like an ally, insofar as it had helped conduct anti-Soviet operations in Afghanistan. No one at the time paid much attention to the Islamist narrative that inspired the so-called mujahadeen, nor to the pseudo-fatwas issued by al-Qa'ida leaders. Moreover, because they were not linked to KGB, Western intelligence agencies concluded they could not be a serious threat. More precisely, they were not perceived as a threat because they did not fit KGB model, reflected first in the organization of CIA and, through NSA, in Canadian SIGINT operations as well. Thus the conclusion reached by Western intelligence after the end of the Soviet Union was that the threat environment had been mitigated. In fact, it had merely changed. The world was not safer, just different. That Western intelligence organizations did not see what had happened, the 9/11 Commission said, was the result of a failure of imagination. That was perhaps understandable on 10 September, but not on 12 September.

As noted in the first section of this paper, imagination, not following a bureaucratic process, is what is needed for effective information analysis; it is imagination that turns information into intelligence. The grave problem faced by Western intelligence agencies dependent on the United States is that they are tempted to solve analytical problems by technical means rather than relying on skill and insight (Codevilla 1992; Friedman 2006). This is not the first time advanced technological means and methods of intelligence collection have been unable to defeat comparatively primitive equipment. As Anthony Cordesman notes, such failures constitute:

a grim warning about trying to rely on military technology as a panacea and the benefits of the revolution in military affairs or force multipliers. In far too many cases, we will find that even when such tools allow us to “defeat” the military forces of an “enemy,” they cannot solve the problem. In other cases, there will be no “enemy,” the war will be of too low intensity for such tools to be effective, or the struggle will be too politically complex. (2001, online)

Despite the overwhelming superiority of American technology in intelligence platforms, the 11 September attacks demonstrated the limits of technical means of intelligence gathering and the importance of human sources. Likewise the ease with which “major combat operations” were concluded in Iraq in 2003 and the persistence of a post-invasion, asymmetric, guerilla insurgency points to the absence of reliable human intelligence, notwithstanding the unsurpassed availability of technically acquired intelligence. In short, SIGINT, upon which the United States has come to rely, has a high yet limited value. Such general and often ambiguous intelligence can provide an overview of ground forces or communications and indicate where further intelligence operations must take place, but it fails to provide a complete picture even where conventional main force conflict is concerned. These conventional observations with respect to American-source SIGINT apply even more strongly to Canada which, as noted, is a net importer of such intelligence.

The value of SIGINT is especially crippled when targets utilize alternative communication means such as dead drops, one-time pads, and anonymous internet proxy servers, all of which are undetectable by ECHELON. American and Canadian capabilities were built to listen in on the Soviets, a lumbering empire that relied on a comparatively primitive communication technology. Spies and terrorists can now exploit the revolution in the global communications industry such as digital cellular phones, sophisticated encryption capabilities, fiber optic communications, and steganography, all of which reduce the effectiveness of signals intercepts. Even conventional SIGINT raises its own unique concerns for intelligence analysts: filtering out signals from noise. This has become a momentous task even for military decisions given the enormous amounts of

raw data collected by American and Canadian SIGINT agencies. Michael Handel and John Ferris describe the difficulty of the modern commander attempting to isolate accurate intelligence:

Contemporary commanders may face a situation unprecedented in history. Intelligence and communications have improved but so have the speed of battle and the need for quick decisions. More information is available more rapidly on more subjects. One thing not changed is the speed required to make human judgements and decisions. Commanders need far more information on a far greater range of matters than in the past. Once, most pieces of intelligence were false but now, they may be true but trivial in quality and overwhelming in quantity. More can be worse. (1995, 49)

Given the overabundance of technically acquired intelligence and other sources of information, the commander or leader is inundated with “noise,” and the major problem remains the determination regarding which is the significant information. Modern intelligence agencies are so deluged with information that they often become paralyzed trying to sift the relevant data from the trivial, creating a new form of Clausewitzian friction: uncertainty based on the overabundance of intelligence (Gladwell 2005, chap. 4). In one sense, this is nothing new: the analysis of information rather than its acquisition has always been the more important task. On the other hand, the vast amount of technically gathered intelligence (and technical efforts at analysis) often exacerbates the perennial problem. In 1965, for example, Eayrs estimated that the Canadian government was able to process and use less than 10 per cent of the data collected by Canadian security and intelligence agencies (Eayrs 1965, 184). The Canadian analytic community can process much less today. Worse, any intelligence collected by Canadian signals intercepts is turned over to the United States for further investigation. This poses a particular problem because Canada has an under-developed analysis community: the vast majority of raw SIGINT data intercepted by Canada is sent to the NSA’s headquarters in Fort Meade. From this mass of raw information, American analysts extract information they think may be of interest to Canada. For their part, Canadian intelligence officials must hope that their American colleagues can sort the wheat from the chaff. Because Canada has no capacity to conduct covert foreign intelligence operations and little analytical capacity, whether for SIGINT or for any other kind of intelligence, it necessarily falls to the Americans to build an analytically meaningful picture from Canadian SIGINT that they then can choose to share or not.

The effect of this new context for Canadian SIGINT is what makes the CSE contributions less valuable to Canada’s UKUSA allies. It is clear that Canada will never possess an intelligence organization with the global coverage of CIA. The enormous financial and bureaucratic costs needed to achieve “information superiority” are prohibitive. However, Canada can attain a more modest “knowledge superiority” – the ability to confirm that information is correct and designed for its own purposes (Campbell 2001). Knowledge superiority can be achieved through nationally directed foreign intelligence collection, backed by a method of corroborating shared intelligence and an improved analytic capability. Currently, even knowledge superiority is impossible because the information Canada receives comes from the United States, and Canada cannot verify its accuracy.

It is a truism that no intelligence organization can function entirely on its own, since no single source can provide a complete picture of any situation. Canada will still need intelligence sharing alliances and the requirement to make contributions to them will continue. However, it must ensure that it can meet its intelligence needs with its own collection and foreign-supplied intelligence. These needs are defined by actual current and future threats to Canadian national security, a discussion of which follows.

4 (e) Threats to Canada

4 (e) i. Terrorism

As noted above, the end of the Cold War created a new and evolving set of intelligence problems. The military threat of the former Warsaw Pact nations vanished, but the threat of terrorism increased. In 1998, CSIS Director Ward Elcock told the Special Committee of the Senate on Security and Intelligence that, “with perhaps the singular exception of the United States, there are more international terrorist groups active [in Canada] than any other country in the world” (Canada 1999b). The annual *Public Report* produced by CSIS beginning in the late 1990s confirmed that terrorism is its chief security concern. The 1998 report, for example, noted the high level of terrorist activity within Canada: “the Counter-Terrorism Branch of CSIS is currently investigating more than 50 organizational targets which embody over 350 individual terrorist targets” (Canada 1998a, online). In 1999, the *Special Senate Committee on Security and Intelligence Report* stated that “Canada remains a venue of opportunity for terrorist groups: a place where they may raise funds, purchase arms and conduct other activities to support their organizations and their terrorist activities elsewhere” (Canada 1999b, online). The committee heard confirmation that most major international terrorist organizations have a presence in Canada. Likewise, the 2000 CSIS document *International Terrorism: The Threat to Canada* outlines the activities of international terrorist and transnational criminal organizations in Canada, including fundraising, providing a safe haven, and planning terrorist attacks (Canada 2000d).

The direct terrorist threat to Canada is a serious concern for CSIS. Prior to the September attacks in June 2001, CSIS stated that Canadians are more vulnerable than ever to terrorism (Bronskill 2001a A13). Now that many terrorist cells have become dormant in the face of increased intelligence and investigative activity, the collection of intelligence will be even more difficult in the absence of a foreign intelligence capacity. The principle of “forward engagement” applies as much to interdicting terrorists as it does to shooting down hostile bombers. Indeed, the notion of “homeland defence” is already surrounded by an aura of defeat because the whole point of war is to make the enemy defend his homeland. This is a major problem with a terrorist network such as al-Qa’ida, which operates more from a virtual base than an actual territory (Cooper 2004b, 158ff). Because such terrorists are largely invisible, however, so too are their manoeuvres towards their next targets, thus indicating the need for an offensive and proactive strategy of engagement. Given the limited foreign mandate of CSIS, however, and the fact that it is already fully occupied in detecting terrorists in Canada and assisting Immigration Canada and Canadian Border Services with “forward screening” (Canada 2003d), expanding CSIS’ mandate would be a mistake. Such an expansion would add to its already significant burdens and create new tensions in its relationships with other intelligence agencies abroad as well as with the RCMP. For reasons indicated in the next section, overseas terrorism would better be investigated by an independent foreign intelligence agency.

4 (e) ii. Economic Espionage

Direct military threats to Canada have vanished for the most part, but indirect military and espionage threats persist in a new form. Competition among states has become less military and more economic. Whereas states previously engaged in espionage primarily for military and foreign policy purposes, intelligence operations now concentrate more on conducting, or guarding against, economic espionage. In 1998, CSIS estimated that agents from twenty-four countries were engaged in state-sponsored corporate and economic espionage in Canada (Livesey 1998). Canada’s advanced industrial and technological society combined with its expertise in certain

sectors, for example, telecommunications, agriculture, and fisheries, make Canada attractive to economic spies. Factors that create vulnerability include the level of foreign ownership in Canada's economy, the number of multinational corporations with operations in Canada, and the number of foreign students studying in Canada in the basic and applied sciences.

In 1999, CSIS identified several sectors of the Canadian economy as sensitive and as likely targets of foreign interest, including: aerospace, biotechnology, chemicals, communications, information technology, mining and metallurgy, nuclear energy, oil and gas, and the environment (Canada 2000d). Canada's economic interests are vulnerable to clandestine collection by visiting foreign scientists, exchange personnel, delegations, business personnel, and members of émigré communities in Canada. Many foreign governments, including some of Canada's allies, direct their state-owned corporations and intelligence services in economic espionage against Canada (Canada 2001b). Press reports and official statements have indicated that the government of the People's Republic of China routinely practices economic espionage in Canada. As one Chinese defector put it, Canada has "soft ribs," meaning that its sensitive political and economic organs have little protection (Freeze 2007).

Economic counter-espionage can be improved by utilizing information acquired from foreign sources to assist domestic operations. Certainly, the United States uses foreign intelligence in its economic counter-espionage operations. One of its primary methods for identifying and countering foreign economic espionage is counter-intelligence. Even prior to passage of the USA Patriot Act, CIA routinely informed the FBI and other government agencies when it learned, via foreign counter-intelligence and economic intelligence operations, about a foreign government or company targeting an American industry. It also informed the State Department and other appropriate American government agencies of instances of economic espionage or state-supported trading practices such as the bribery of contracting officials. Conversely, the counter-espionage programs of CSIS are hampered by the lack of foreign information about hostile countries that can be collected only through counter-intelligence operations abroad. The ability to gather foreign counter-intelligence would supplement domestic efforts to detect economic spies in Canada as well as activities hostile to Canadian economic interests overseas, thus making Canadian counter-espionage operations far more effective.

4 (e) iii. *State-sponsored Espionage*

Traditional espionage from hostile state-based intelligence organizations also remains a danger. In its 2000 threat assessment, CSIS stated that "intelligence services of certain foreign governments continue to clandestinely collect information considered to be in their national interest and to engage in foreign-influenced activities within émigré communities" (Canada 2000d). Foreign intelligence officers have been directed to collect information on issues such as trade negotiations and military and technological developments. CSIS anticipated that some of these intelligence services would expand their activities and it forecast an increased threat to Canadian interests, particularly from traditional rivals Russia (Trickey 2001) and China (Canada 2000a).

Clearly, foreign espionage, economic espionage, and terrorism continue to threaten Canada (Canada 2003d). These threats emanate from abroad, yet Canada has no eyes and ears abroad to monitor them until they reach Canadian shores. Although SIGINT is useful for gathering external intelligence, it can only provide a partial picture. HUMINT is also necessary to determine capabilities and hostile intentions towards Canada that CSE cannot intercept.

5. WHY CANADA NEEDS A FOREIGN INTELLIGENCE AGENCY

Without an expanded foreign intelligence capacity, Canada's ability to meet both its international obligations and possible espionage threats to its national security is impaired. The scale of the problem can be demonstrated by comparing Canada's intelligence requirements to its current intelligence community. These requirements fall into four general areas: political intelligence, economic intelligence, defence intelligence, and alliance contributions. Once Canadian intelligence requirements are made explicit, the need to develop a foreign intelligence capacity is obvious.

5 (a) Canadian Intelligence Needs

5 (a) i. *Political Intelligence*

The relationship between intelligence and foreign policy is intimate and essential. It is impossible to implement military, economic, or political strategy without accurate intelligence. Foreign policy priorities – whether they result from ideological agendas, parochial interests, or perceptions of national interest – help define the information that the intelligence community is called upon to collect and analyze. For example, DFAIT states that one of its three key foreign policy objectives is, “the protection of [Canadian] security within a stable global framework by using diplomacy to protect against military threats, international instability ... international crime, uncontrolled migration, and the spread of pandemic diseases” (Canada 2002b). Without independently collected foreign HUMINT and a competent analytic capacity, DFAIT cannot formulate a coherent policy and is thus unable to fulfill its mandate effectively.

Active foreign policy benefits from effective foreign intelligence. The British, for example, have long justified maintaining an effective foreign intelligence establishment to support its participation in international politics (Hermann 1996). By the same token, because Canada is active internationally as a member of NATO, the Organization for Security and Cooperation in Europe (OSCE), the G8, La Francophonie, and the Organization of American States (OAS), to name but a handful, it also needs foreign political intelligence. As noted above, this need is even more critical with respect to Canada's international peacekeeping contributions. The end of a bipolar world increased the instability of the global security environment, thus the need for timely awareness of how foreign events will affect Canadian interests has been enhanced. Furthermore, Canada has committed itself to fighting terrorism alongside the United States, its NATO allies, and the United Nations, even though it does not have the security and intelligence capacity to fulfill that pledge. Without taking steps to develop one, Canada's future contributions will be as hollow as those of the recent past, thus adding to the damage done to Canada's international reputation and creating more dependence on the United States (Cohen 2003).

The proliferation of weapons of mass destruction (WMD) continues to be a leading international concern. The 2000 *CSIS Public Report* cites states such as North Korea, Iran, Iraq, Libya, and Syria as posing a threat to international, and therefore Canadian, security. The 2003 report did not identify countries that posed a danger, but it did note the problem that al-Qa'ida armed with WMD would pose. CSIS also acknowledged that the intelligence services of certain foreign governments remain active, targeting dissidents associated with long-standing regional or political conflicts who currently reside in expatriate communities in Canada. Similarly, politically motivated violence remains largely an extension of overseas discord. Extraordinary domestic and international collaboration is needed to combat international terrorist groups that use Canada as a base from which to orchestrate their activities abroad. Without a foreign HUMINT complement

to its domestic security intelligence programs, Canada will remain a defensive, passive, and soft target, able only to react to threats, not prevent them from developing.

Other political issues require intelligence support. Canada remains a world leader in accepting refugees and immigrants, including a steady flow of people from regions of strife. Some bring the politics of conflict with them. Immigration Canada has acknowledged that it cannot clear the backlog of hundreds of top-secret immigration applications and was compelled to recruit a private consultant to review the glut of immigration files accumulated since 11 September (Blackwell 2002). A liberal immigration policy coupled with a poor security process brings inherent dangers to Canadian national security from so-called failed states, that is, countries that disintegrate as viable political and constitutional entities, the governments of which lose their ability to ensure public order. Security threats can occur if the militant fringe of the émigré community endeavors to replicate or support the homeland dispute in Canada (Thompson and Turlej 2003). Foreign intelligence collection, as well as the collection of security intelligence in foreign parts, is necessary to investigate these threats.

CSIS has long acknowledged that many of Canada's security preoccupations originate abroad. These issues touch on high politics in many different ways. In 2002, for example, CSIS reported that Iraq, Iran, and North Korea were aggressively trying to develop nuclear weapons, a significant but highly controversial claim (Bell 2002b). Since most of Canadian foreign intelligence comes from the United States, this evidence presumably also derived from American sources. Without an independent means of confirming such information, Canada accepted American-supplied intelligence uncritically, even though it proved to be highly questionable with respect to Iraq. Canada refused to take part in the Iraq invasion, but it did not base its refusal on any intelligence that might have called the American analysis into question (Goldenberg 2006). Lacking a foreign intelligence capacity upon which to base its decision, the action taken by the Chrétien government appeared arbitrary in the extreme. As a result, Canada-United States relations were badly strained. If Canada could point to sources of intelligence other than those supplied by the United States or other than the even more questionable political judgement of United Nations bureaucrats, the damage would unquestionably have been reduced.

As long ago as 1996 – halfway between the end of the Cold War and 9/11 – the auditor general's report entitled *The Canadian Intelligence Community* discussed several potential problems that might have serious political implications for Canada (Canada 1996a). These included: a) international terrorism conducted against the United States; b) a Canadian resident involved in the planning, financing, and arming of an international terrorist group about to commit a terrorist act overseas; and c) political instability overseas affecting Canadian nationals abroad (Canada 1996). These hypothetical situations were all later realized by: a) the 11 September terrorist attacks; b) the 1999 arrest of Ahmed Ressam, the “millennium bomber” who was detained after getting off a ferry from Victoria en route to bomb LAX; and c) the 1998 evacuation of Canadians from Jakarta because of political violence under the Suharto regime, or the 2006 evacuation of Canadians from Lebanon during the conflict between Israel and Hezbollah. The report also suggested the need to shift from one primary intelligence target – the former Soviet Union – to a broader range of targets that requires political, economic, and social intelligence. A foreign intelligence service would improve Canadian domestic security intelligence by providing advance warning of potential threats to national security. In itself, this would benefit Canadian diplomatic and strategic interests significantly. Perhaps even more important was the recommendation of the auditor general to strengthen leadership and coordination through senior-level guidance to, and review of, intelligence gathering coupled with explicit direction with respect to national priorities. By and large, the response of the intelligence community was to endorse the report. In effect, the affected parties were asking for greater direction concerning the job they were tasked with

performing, namely the production of intelligence. The implicit criticism is likewise obvious: the government of Canada did not really know what it wanted to do with its own intelligence capability, however modest.

5 (a) ii. *Economic Intelligence*

DFAIT does not conduct any kind of covert intelligence gathering. This has negative implications for protecting Canadian security. The need for business and competitive intelligence about foreign markets is growing (Farson 1999). For any Canadian exporter seeking to enter a foreign market, methodical and organized intelligence is an obvious necessity. A great deal of market intelligence is available from open sources, but unlike Canada's major trading partners and competitors, government-sourced information, which may or may not prove useful in any specific instance, is available only from open sources. Under some circumstances, on-going covert monitoring and surveillance of the commercial activity of competitors is prudent. Foreign intelligence services, through their unique collection capability, can provide valuable economic intelligence unavailable via other means (Porteous 1995).

Although the Canadian government has made no official statements about offensive economic intelligence, indications from parts of the Canadian intelligence community point to an increased interest in the economic and commercial world (ibid.). The need for such market intelligence prompted DFAIT in 1997 to create the Market Research Center to provide a quick snapshot of the opportunities in a specific market for a specific product or service. However, the newly formed Market Intelligence Division assisting DFAIT is limited to gathering market intelligence and information from open sources. A foreign intelligence service, among other activities, can help monitor member state adherence to international agreements affecting national economic and commercial interests, which is why, for example, CIA pursues foreign corrupt practices, as does the Australian Foreign Intelligence Service. However, because DFAIT has limited assets specifically assigned to open-source economic intelligence, their collection activities are of limited value. A foreign intelligence service could gather information to block potential losses by providing economic intelligence through the covert monitoring of trade agreements, unfair trade, and other sharp practices.

In an increasingly globalized marketplace, DFAIT's limited intelligence capability puts Canadian businesses at a disadvantage; other industrialized nations do not shy away from using their offensive intelligence capabilities to promote the interests of their flagship companies (Sevunts 2000). In 1999, CSIS outlined the damaging effects of economic espionage on Canadian interests in the forms of lost contracts, jobs, and markets, and of an overall diminished competitive advantage (CSIS 1999). CSIS stated that leading-edge technology, research and development, and other sensitive business information are currently being targeted by foreign governments. Canada must protect those technologies that are integral to its economic interests. Without advance warning of what interests are being targeted, Canadian economic intelligence is entirely passive. A foreign intelligence service collecting open source *and* covert economic intelligence would assist in the overseas detection of such hostile operations and boost Canada's economic interests.

5 (a) iii. *Defence Intelligence*

Defence intelligence will continue to be a priority for Canada as it engages in multilateral peacekeeping, peace enforcement, and stabilization operations with the United Nations and

NATO, despite significant cutbacks over the past decade and a half and the more recent budget restoration. Military intelligence has been particularly degraded. As a 2001 *National Post* headline put it, “Budget Cuts Hurt Our Ability to Spy, Forces Chief Says” (Pugliese 2001). As a result, the capacity of the J2 Intelligence Directorate is extremely limited because there are few military attachés posted abroad to collect defence intelligence. As noted above, the Canadian intelligence failures in Congo, Rwanda, Somalia, and the former Yugoslavia demonstrate both the need for accurate defence intelligence and Canada’s inability to obtain it. Because Canada will continue to deploy with multinational coalitions in the future, it must either improve its intelligence capability to support future deployments or it will repeat past intelligence failures.

Moreover, the two “fusion centres” established to develop the Canadian Forces Intelligence, Surveillance, and Reconnaissance (ISR) program to receive, process, analyze, and distribute intelligence rely heavily on technically acquired rather than human intelligence, and thus are burdened with all the familiar limitations of SIGINT and communications intelligence, COMINT (CASIS 2002). Likewise, the approval of a Nuclear, Biological, and Chemical (NBC) Response Team by DND is a positive development (Blanchfield 2002; Barber 2001). However, as noted above, because the Canadian Forces has an inadequate intelligence infrastructure, any future development of a rapid response unit, which is heavily dependent upon accurate and current (or “actionable”) intelligence, is highly questionable. Like other Canadian military units, the NBC response unit will have to wait until shared intelligence filters down the chain of command from friendly foreign agencies. A Canadian foreign intelligence agency would be tasked to collect needed information and disseminate it prior to and during deployments. Defence intelligence is essential for Canadian Forces deployments. These deployments represent significant foreign policy tools, and a reduced defence intelligence capability will significantly degrade one of the primary foreign policy instruments available to Canada.

5 (a) iv. Alliance Contributions

Finally, alliance contributions and intelligence sharing will present challenges for Canada in the next decade. Canada is party to more than 200 national security and intelligence agreements. It co-operates with the intelligence agencies of more countries than ever before and has consequently acquired increased intelligence obligations. All the members of the UKUSA intelligence alliance, Canada included, failed to anticipate the September 11 terrorist attack, and all failed to warn. After 11 September, the United States intelligence community undertook a massive review of its capabilities and limitations. On 26 September 2001, Jim Gibbons, chair of the American Select Intelligence Human Intelligence, Analysis and Counterintelligence Subcommittee, stated that

unfortunately, the United States did not have HUMINT on the plans and intentions of the group that committed the recent atrocious terrorist attacks. To protect our national security and the lives of millions of civilians, we have to improve our HUMINT capabilities. No amount of aircraft, ships, troops or satellites can protect us, if we do not know whom [sic] the enemy is, where he is and what his next move may be. Terrorists are becoming increasingly more sophisticated and are able to avoid our technical surveillance. Thus, it is imperative to reinvest in HUMINT, an area of our intelligence community that has been downsized since the end of the Cold War. (2002, online)

Similarly, following a decade of cutbacks, MI6 is seeking to double its recruitment of front-line officers to resolve its inability to conduct effective counter-terrorism operations (Beaumont and

Rose 2002). Canada has made no effort to develop such a capability. Instead, it is bolstering an intelligence system that has already been proven ineffective. Without an independent foreign HUMINT capacity, Canada will be less able to play a role in global intelligence and maintain its place at the allied intelligence table. If Canada does not undertake serious changes to the structure of its security and intelligence community, it will soon enough be seen by its intelligence partners as unworthy of the status of ally (Wark 2001). Canadian capabilities and efforts during the Second World War and the Cold War gave the country a place in international intelligence alliances, but that system of intelligence sharing is gone. Serious and imaginative efforts, along with a significant financial commitment, are now needed.

In late 2001, the Office of the Solicitor General announced that \$35 million would be spent to enhance analytical support and to facilitate the exchange of intelligence and investigative support with other law enforcement and intelligence partners (Canada 2001a). Art Eggleton, then minister of national defence, stated that

these additional resources, coupled with the *Anti-Terrorism Act*, will better position [Canada] to contribute to the international campaign against terrorism [and the resources] will also be welcomed by our allies as evidence that we are committed to remaining an active and contributing member of our close intelligence partnerships. (Canada 2001a)

Eggleton's remarks indicate that there is a political awareness that Canadian intelligence capabilities need to be improved. Unfortunately, by refusing to expand collection capacity as well, the government decided to reinforce failure. At the very least, it is self-evident that in order to share intelligence, it is necessary to have something to share.

Since the end of World War Two, Canada has resisted the idea of a foreign intelligence service. In discussing the history of intelligence in Canada and the problems the Canadian intelligence community has faced, the argument is also implicitly made for establishing a foreign intelligence capacity. Those disputes can be summarized according to three categories: problems with intelligence sharing, information sovereignty, and national protection. Before summarizing them, the arguments against establishing a Canadian Foreign Intelligence Service are reviewed.

5 (b) Foreign Intelligence: Arguments Against

5 (b) i. Cost Prohibitive

The fundamental argument against the establishment of a Canadian version of MI6 is cost. While the budget for Britain's MI6 is incorporated into a total for all British intelligence activities, the *British Intelligence and Security Committee Annual Review* put the intelligence budget for 2001–02 at 876 million pounds, with some 150 million pounds allotted to MI6 (Great Britain 2002). The figure for the American CIA is even more impressive. In response to a Freedom of Information Act lawsuit brought by the Center for National Security Studies in 1997, Director of Central Intelligence George Tenet announced that the CIA budget for 1997 was \$26.6 billion (Levin 1997), and the 2004 estimates are around \$40 billion (Bendetto 2004). Canada cannot come close to allotting such funds for a foreign intelligence service, especially given the post-September 11 infusion of capital into Canada's security intelligence infrastructure. The failure of American intelligence services to predict the September 11 attacks and the questionable intelligence regarding WMD prior to the invasion of Iraq led many to argue that any expenditure on foreign intelligence would be pointless. CSIS has argued that, compared to the United States, the direct threat of terrorism to Canada is low, and that Canadian foreign intelligence activities

might have the effect of making Canada a target for extremist groups determined to counter covert operations. The conclusion? The costs of establishing a Canadian secret service would outweigh any potential benefits.

The government conventionally maintains that Canada's existing intelligence sharing agreements are cost-effective, especially when compared to the projected cost of a Canadian secret service. In a memorandum to the parliamentary committee reviewing the CSIS Act in 1990, the radical Law Union of Canada spelled out the main objection to a foreign intelligence service: "we doubt in these times of economic restraint, sufficient resources will be available to provide anything but holiday type assignments for the few intelligence agents placed in the field. We doubt the quality of information will justify any such expenditures" (Law Union 1990). Operatives charged with managing foreign intelligence networks abroad would require expensive and specialized training as well as seed money for new equipment, expenses, and agents separate from that received currently by CSIS members in their domestic security role.

5 (b) ii. *Inexperience*

Canada has previously met with only limited success managing major security and intelligence operations such as the Air India bombing. To expand CSIS's foreign intelligence mandate might seriously add to the agency's existing problems. Personnel operating abroad would have to be under diplomatic cover, critics argue, and years would be needed to slot people in so as not to raise suspicions among host governments, to establish effective espionage networks, and finally, to produce usable intelligence. Even if raw information were collected overseas, finished intelligence would not be ready for consumption overnight. Given its current analytical capability, the Canadian intelligence community could not collate and process new information in a timely manner. Without a trained cell to assess raw information, any money spent on collection would be wasted. Perhaps even more significantly, the government has proven itself a poor consumer of intelligence. Even if Canada developed a foreign intelligence service and an analytic cell, if the government does not improve its ability to use intelligence, it will be useless.

5 (b) iii. *Reputation*

Canadian political leaders have long claimed to enjoy an exalted reputation as a "middle power" able to deploy globally on behalf of the United Nations. This reputation followed from the claim that Canada has no hostile intentions towards other states. The creation of a covert foreign intelligence service would detract from that reputation, making it difficult to participate in multilateral negotiations or deployments. Canada could no longer claim to be the world's favourite "honest broker." Others have argued that because Canada is opposed to foreign espionage activities on its soil, to operate clandestine espionage rings in other countries would be hypocritical. The latter argument is a variation of the "honest broker" position.

In 1993, SIRC published a redacted *Counter-Intelligence Study* which examined the pros and cons of a Canadian foreign intelligence service. Among its concerns was the potential lack of Canadian direction for targeting, the propensity for such an agency to become a subsidiary of the American CIA, the loss of reputation abroad merely by having a service, and the inevitability of failures (Canada 1995). The objections raised to the idea of a Canadian secret service vary in significance and coherence, but collectively they carry political weight and must be answered in

order to justify such a service (*Globe and Mail* 2007, A12). Let us then summarize the arguments regarding intelligence sharing, information sovereignty, and national protection.

5 (c) Foreign Intelligence: Arguments For

5 (c) i. *Problems with Intelligence Sharing*

Canada relies on its allies for information. Allies share intelligence on specific issues of mutual concern such as al-Qa'ida, but often have little interest in using scarce resources to monitor groups abroad that may be of significant interest to Canada but low priorities for them, for example, the Tamil Tigers. If Canada is to target groups of greater interest to this country than to Canadian allies, it must develop the capacity to do so itself. Similarly, Canadian needs may be affected if the intelligence agencies of other nations retrench owing to their own fiscal constraints, or withdraw from parts of the world because of changes in their national policies and priorities. A Canadian foreign intelligence service monitoring foreign agents and transnational criminal and terrorist organizations would give Canada information of use to itself according to Canadian priorities, and it would contribute to existing intelligence alliances, thus reducing the perception that Canada is an unworthy free-rider.

Since Canadian allies such as Germany and France conduct foreign intelligence operations against Canada, particularly in economic and trade areas, Canada should be equipped to not only counter those activities, but to detect them in advance and respond in kind. A Canadian secret service would make Canada more independent of its intelligence alliances, increase its contributions to them, and demonstrate active commitment to shaping the international order in which Canada wishes to play an influential role.

5 (c) ii. *Information Sovereignty*

The 1999 senate committee noted their concern that “Canada’s needs may not always be given the priority they deserve by foreign intelligence organizations and, furthermore, that the intelligence Canada receives may be filtered through the prism of other nations’ domestic and foreign policies” (Canada 1999b). Foreign intelligence can produce evidence of current foreign penetrations on one’s own side, which means that foreign counter-intelligence is critical to domestic security. Foreign intelligence information about penetrations or interception by other sources such as SIGINT can be used to strengthen domestic security and stop exploitation of those weaknesses by hostiles. Without a foreign intelligence agency, however, Canada can take only reactive, rather than proactive measures.

Similarly, because hostile intelligence services have penetrated the intelligence communities of Canadian allies, accepting finished intelligence from allies can be dangerous. A Canadian foreign intelligence service would improve Canadian ally-worthiness and also be able to confirm the accuracy of intelligence received from allies, vetting not only the product, but also the source. Canada would have an independent ability to collect, analyze, confirm, and disseminate intelligence and be in a position to generate intelligence in support of coalition, NATO, or United Nations operations. Canadian-supplied intelligence would be up-to-date, immediately available, and specifically designed for Canadian use by both civilian and military consumers. A Canadian Foreign Intelligence Service might also help prevent Canada from being marginalized should a binational North American defence command ever be created (Windsor 2002).

Unfortunately, the temptation for the Canadian government to underplay the realities of its strategic partnership with the United States, preferring instead to emphasize Canada's distinctiveness and autonomy with respect to security and defence priorities, is always present. The hypocrisy of Canada's position as a very junior partner in North American defence exacerbates the real problem: as Canada has grown more reliant on America for military and intelligence support, the United States has increasingly looked on Canada as more a liability than a partner in continental defence. This has led to the Americans doing intelligence work for, and in, Canada, and consequently, to a critical erosion of Canadian sovereignty. Canada may be unable to afford to develop the full spectrum of foreign intelligence capabilities. At a minimum, however, it must acquire those capabilities related directly to military operations other than war and to those areas of public policy considered by the government to be critical to its decision superiority.

5 (c) iii. *National Protection*

Canada suffers from a serious lack of training and competence in the conduct of covert operations abroad. Despite Elcock's veiled claims that CSIS conducts covert operations abroad, the question of professional competence is not thereby settled (Bell 2003). If there is no foreign intelligence agency in Canada, who trained CSIS for covert overseas operations when its mandate clearly states that foreign intelligence can be collected only in Canada?

A dedicated Canadian foreign intelligence agency trained by allies specifically for overseas and for covert operations would gather intelligence more effectively than would a domestic agency such as CSIS, whose members are trained for domestic intelligence operations. John Starnes stated in 1987 that "the worst possible situation would be to delude ourselves into thinking we can get into the dangerous business of carrying out covert activities in other countries without getting our hands dirty. We might delude ourselves, but we certainly would not delude our allies or enemies" (4). This would certainly apply to CSIS, which is known globally as a security intelligence service without a foreign collection function. Moreover, such a radical change in mandate might upset the excellent liaison arrangements Canada has with various foreign intelligence agencies that have taken many years to establish. CSIS liaison officers are known as security intelligence officers, and such a change in their mandate would raise suspicions among foreign liaison officers as to what information is being collected and for what reason.

Moreover, recent attempts by the Canadian government to conduct foreign espionage operations do not give one confidence in their expertise. According to the *National Post*, in early 2000, the government approached the aid agency CARE Canada to have its members monitor peace agreements and human rights abuses in Kosovo (Graham 2001). This information was to be passed to the Organization for Security and Cooperation in Europe, of which Canada is a member, as part of its intelligence sharing obligations. In practice, NGO members are often used by security agencies as sources of local intelligence. In this instance, however, because Canada has no trained foreign intelligence operatives, CSIS was unable to instruct the Canadian aid workers it recruited in Canada. None of these civilians had any intelligence training, yet they were expected to produce regular and useful reports. No Canadian foreign intelligence officers were present to act as trainers, handlers, or liaisons, making the job of monitoring difficult and dangerous. Instead of having trained professional intelligence officers running a ring of agents, Canada utilized untrained and unsupervised aid workers in a clandestine intelligence role and violated the neutrality of the non-governmental aid agency, all at the cost of \$3 million to Canadian taxpayers.

The arrest of Edmund Pope over the Squall torpedo fiasco in June 2000 also indicated incompetence in mounting a foreign intelligence operation. The *Washington Post* stated that “Pope fell afoul of an intelligence operation in which he was not involved: an effort by the Canadian government to buy a handful of Russia’s advanced Squall torpedoes from a defense plant in the former Soviet republic of Kyrgyzstan” (Mintz 2001, A1). This article suggested that a clandestine Canadian intelligence operation had been mounted with British and American involvement to purchase the torpedoes; Canada was likely acting as a proxy for its allies. If so, it was spectacularly unsuccessful, and Pope spent nearly a year in a Russian jail.

The subsequent arrest of Igor Sutyagin in Moscow shed even more unfavourable light on Canadian intelligence. The Russian security agency, the FSB, alleged that Sutyagin was a Canadian spy who attempted to gather secret information about Russian nuclear submarines and the Squall torpedo (York 2000). Sutyagin was never proven a spy, although he had taken part in a study of civil-military relations in Russia funded by the Department of National Defence (Flynn 2001). Whether Canadian intelligence or military officers were involved with Sutyagin, perhaps the most telling comment on Canadian involvement with the Squall operation was a statement by the American government that “with the Canadian deal dragging on for years, the Navy could not have warned all Americans to avoid inquiring into Russian maritime matters at that time. The Canadians never provided real-time tactical information about where their effort stood” (York 2000). It has never been unambiguously determined whether Canada was involved in any of the espionage operations involving the Squall torpedo; if so, it was highly uncoordinated.

5 (d) A Problem Restated

If Canada cannot fulfill its intelligence requirements, it will lose a competitive advantage for its foreign and domestic security. More significantly, it risks being marginalized by the United States in continental security agreements. Canada’s intelligence assets have historically proven inadequate to meet its national needs, and without an expanded foreign intelligence program, it is unlikely that these growing needs can be met. The obvious solution to Canada’s intelligence deficit is the creation of a foreign HUMINT service, which means the objections raised above and problems with CSIS must be addressed.

The most common argument against a Canadian foreign intelligence service, financial concern, is not unresolvable. Defence minister Art Eggleton stated during a 2002 Liberal caucus committee on defence and foreign affairs that “it’s a question of how much we need to do this, how much we need to spend additional taxpayers’ dollars.” The 1993 SIRC study provided an estimate of \$20 million, and as Alistair Hensler notes, this figure took into account the British experience and utilized the CSIS personnel to estimate a dollar amount (Hensler 1995). This conclusion makes no allowance for the different priorities or size of a Canadian foreign intelligence service. It is true that Canada has traditionally borrowed from Britain, but the United Kingdom has had a significant foreign intelligence capacity ever since it was a colonial power, and its global coverage requires a much larger expenditure than a smaller Canadian version would demand. The 1993 SIRC estimate of \$20 million could easily be tripled, and even so, Canada could accommodate the cost. If the political will is present to create CFIS, it is certain that there would be ample funds to establish and maintain it.

As noted at the beginning of this study, the 2006 conservative election platform promised to create a “Canadian Foreign Intelligence Agency to effectively gather intelligence overseas, independently counter threats before they reach Canada, and increase allied intelligence operations.” In the summer of 2006, public safety minister Stockwell Day was considering expanding the role of CSIS

to include foreign intelligence. By February 2007, the urgency to create a foreign intelligence agency seems to have been forgotten by the government (Mayeda 2007b), and by the spring of 2007, the notion seems to have been dropped entirely (Mayeda 2007c, 2007d; Galloway 2007). This change seems likely to have resulted from “administrative capture” of the political leadership of the Public Safety Ministry by bureaucrats in CSIS, much as Department of Finance officials were able to change government priorities regarding income trusts.

Canadian inexperience in foreign espionage is not insurmountable. Using existing liaison arrangements, Canada could reap the benefits of its allies’ experience in foreign espionage by studying with British and American intelligence officials. Utilizing a “train the trainer” program with instruction from MI6, CIA, or ASIS, Canadian intelligence members could return to Canada and prepare new agents, creating the cost-effective option of in-house instruction. The missing HUMINT component, which involves recruiting foreign nationals as human sources and maintaining secret relationships, contains an element of risk, but it is not totally foreign to Canadian intelligence personnel. Canadian police forces, security intelligence services, media reporters, and diplomats have practiced the art of developing human sources for decades. As former Canadian ambassador Norman Spector stated, “establishing a foreign [intelligence] service would give us something to trade and leverage in future dealings with [the United States]. Though human intelligence is dangerous work, our sizable immigrant population, benign international reputation, and desirable passport give us a comparative advantage” (Spector 2002, A14). More specifically still, there are over 200 ethnic groups in Canada, and the “visible minority” population is growing at nearly five times the rate of the total population. This human resource provides a significant opportunity to recruit linguistic talent (Beare 2003), a point also made by Rudner in his senate testimony (Canada 2003a). Given the chronic shortage of translation skills among Canada’s allies, Canada’s multiculturalism policy can also be a security asset (Canada 2003a). In other words, Canada’s relative inexperience with foreign intelligence could be reduced quickly and significantly.

Nor would espionage damage Canada’s reputation. First of all, Canadians have spied for friendly countries (O’Neill and Fisher 2007). Second, the record of expelling each other’s personnel for real and alleged acts of espionage throughout the height of the Cold War produced no long-term adverse impact on relations between opposing parties. More recently, there was little permanent reaction by the Chinese government after discovering twenty-seven listening devices in an American-supplied Boeing 767 provided for Chinese president Jiang Zemin. The Squal torpedo incident did not damage Canada’s bilateral relations with Russia. Other incidents, however, have caused embarrassment for Canada’s security intelligence community. American newspapers such as the *Boston Globe* sensationalized the loss of sensitive documents by CSIS in the 1990s. “In Canada,” the newspaper reported:

secret agents may find themselves sifting landfills for lost secrets amid one of the worst spy scandals in the country’s history. The Canadian Security Intelligence Service is now confirming that a top-secret document ... was stolen from the back of a spy official’s minivan last month. The culprits are believed to be smash-and-grab thieves, not secret agents from enemy powers. The incident has triggered a huge political controversy and damaged the reputation of the Canadian Security Intelligence Service. (Nickerson 1999, A4)

The distinction between Canadian, American, and British citizens is also diminishing in international relations. Canada is a close ally of the United States and of Britain, a fact well known to the world. Canada is equally well-known as a middle power and for being intimately allied with the United States and thus far from neutral. Although a direct attack against Canada is not considered likely, the country has been identified as an al-Qa’ida target. Canada has unquestionably

been a safe haven for fundraising, for weapons purchases, passport forgery, hiding out, and organizing operations against the United States (Bell 2004). Given Canada's military and intelligence dependence on the United States, it is also well known as a country highly reliant on its allies for foreign intelligence. Its military reputation has suffered in the last decade and a half as a result of substantial cuts to the defence budget, and Canadian intelligence has suffered similar cuts. The issue of restoring a foreign intelligence service, however, is far from resolved, notwithstanding recent increases in military CSE and CSIS budgets (Bronskill 2005).

6. CFIS

The two obvious ways to solve Canada's intelligence problems are to reform existing institutions or to create a new foreign intelligence service, CFIS. Many advocates of an expanded Canadian foreign human intelligence capability (including, most recently, the Harper government) have suggested expanding CSIS's mandate to include foreign intelligence abroad, so this possibility is examined first.

6 (a) CSIS – Spycatchers and Spies?

Expanding the mandate of CSIS looks like the natural choice for a new Canadian foreign intelligence service. It is a proposal that has received intermittent governmental support over the years. SIRC's 1990 report *In Flux But Not in Crisis* recommended that Canada's foreign intelligence needs be met by removing the words "within Canada" from section 16, allowing CSIS agents to collect foreign intelligence abroad (Canada 1990a). There are good reasons why CSIS could be considered the home of a Canadian foreign intelligence service, but better reasons to keep the two agencies separate.

CSIS claims to be involved already in intelligence activities abroad and claims to have a cadre of trained and experienced intelligence officers who conduct liaison operations abroad as well as analysts within the Research, Analysis, and Production (RAP) section of the agency to analyze raw intelligence. Creating a new foreign intelligence directorate within CSIS would obviously be less costly than establishing an altogether new service. Since CSIS members are already involved in the Security and Intelligence Secretariat of the Privy Council Office, expanding existing assessment and coordination structures looks attractive. A change to the CSIS Act would also be politically easier than the creation of an entirely new service with a new mandate. According to Peter Russell, a simple amendment to section 16 of the CSIS Act would end the legal constraint on the ministers of National Defence or of Foreign Affairs should they wish to have CSIS collect information abroad about the capabilities, intentions, or activities of foreign states (Canada 1988). There are, however, stronger arguments against an expansion of CSIS's mandate.

6 (a) i. *Why Spycatchers and Spies Should Remain Separate*

CSIS is accountable to the solicitor general, who is responsible for protecting Canadians and helping to maintain peace and safety in Canada. This department has little use for, or experience with, foreign intelligence. CSIS collects "foreign" security intelligence chiefly at the request of bureaucrats in DFAIT and DND, not by ministerial direction. It would therefore be a violation of parliamentary conventions regarding ministerial responsibility to assign foreign intelligence to a ministry with so little concern with the foreign intelligence product. Certainly the "corporate culture" of CSIS would have to be fundamentally changed to accommodate the complexities, ambiguities, and sophistication required to undertake international intelligence-gathering, which is to say, stealing secret information. CSIS remains largely a parochial organization that still draws a great deal of its operating ethos from the RCMP that preceded it (Campbell 2001). A new approach is needed for a foreign HUMINT capacity, and CSIS is probably not the best environment to nurture such change.

The differences between security intelligence and foreign intelligence are not just cultural, but also legal, operational, and methodological (Hulnick 1997). As Stewart Baker noted, "combining

domestic and foreign intelligence functions creates the possibility that domestic law enforcement will be infected by the secrecy, deception, and ruthlessness that international espionage requires” (1993–94, 37). In fact, Baker understates the problem. Of course there is always the “possibility” that domestic law enforcement will become “infected” with “secrecy, deception and ruthlessness.” The point is that foreign intelligence effectively requires such attributes so that housing foreign and security apparatuses within the same organization practically ensures such an “infection.” Only when the entire enterprise is extra-legal, as the KGB notoriously was, does the combination of domestic and international security cease to make much of a difference.

Security intelligence collection by CSIS is presently focused on Canadians, landed immigrants, and other residents of Canada who pose threats to national security. The checks and balances of the CSIS Act are designed to protect the rights of all persons under the scrutiny of CSIS. Because it operates almost entirely within its borders, CSIS is also bound to operate within the laws of Canada. In contrast, foreign intelligence involves recruiting secret sources by whatever means necessary (not all of them exemplary, or even legal) in foreign governments, terrorist organizations, and commercial sectors to obtain political, military, or economic intelligence. This is not, and should not be, a role undertaken by an agency whose purpose is closer to enforcing than to bending or breaking the law. That was, after all, the most important lesson learned from the original scandals within the RCMP Security Service that led to the creation of CSIS. There is no need to learn that lesson again or to repeat the errors that made it necessary to learn in the first place.

These operational and methodological differences result from the different purposes of each type of organization. Foreign intelligence agencies target sources through covert or clandestine means and seek non-public, or secret, information about foreign governmental policies and about the activities of foreign agents and other spymasters. Security sources are often deployed against single criminal events or activities and may provide intelligence that is then passed on to law enforcement agencies. In such cases, the rules of legal disclosure apply, including methods of investigation. While CSIS is not a law enforcement agency, it works closely with the RCMP, is bound by the same legal constraints as the RCMP, and gathers security intelligence that is typically turned over to the Mounties for action. The problem of “cops and spies” is exacerbated by the already strained relationship between the RCMP and CSIS. CSIS sometimes maintains that security intelligence is not evidence because of the manner in which it is collected and because the rules of disclosure governing criminal acts are not applied. In fact, however, those rules must apply equally to the RCMP and to CSIS if ever there is to be a criminal action brought against a security threat in open court.

This issue was publicized when two CSIS agents were called as witnesses in the trial of Mourad Ikhlef, an accomplice of Ahmed Ressam. In spite of objections by government lawyers, Mr. Justice Pierre Blais ruled that CSIS agents must take the stand, citing that “if [I] accepted the argument, agents of the Canadian Security Intelligence Service would never be called to testify ... This could be abusive” (Ha 2001, A10). In contrast, the expectation of foreign intelligence personnel (and occasionally for security intelligence personnel if they are engaged in counter-intelligence work) is not to arrest a source and stop the flow of information but to use arrest as a threat in order to create a controlled agent. In terms of organizational culture, a fundamental difference exists: foreign intelligence agents want to exploit their sources, whereas security intelligence personnel typically gather intelligence that is eventually turned over to police and may be used in court as evidence:

[In court] the source’s identity will eventually be revealed, as well as the methods by which the information was gathered. [Security intelligence] agents have to appear in court to testify and all the information has to be made available to the defendant. Those kinds of procedures are anathema to intelligence officers. Case officers –

handlers – are usually undercover, do not want their affiliations made known, and do not want their sources and methods made public. (Hulnick 1977, 277)

In the American context, these different purposes are reflected in the separate institutions of CIA and the FBI; in the British, between the Secret Intelligence Service (MI6), the Security Service (M15), and Scotland Yard.

The conflict between foreign and security intelligence is not simply a manifestation of bureaucratic rivalry; rather, it stems from a fundamental difference in operations. Consider the following question. In Canada, when a foreign agent is discovered, is that agent turned by CSIS or arrested by the RCMP? Who makes that decision? If the decision is (somehow) made to run an agent, what methods will be used? In part, it depends on the nature of the operation, but also on the agent and lead organization. When CSIS operates in Canada, it is subject to the Charter and to Canadian law. Covert operations conducted overseas are not subject to either. If the same personnel are involved, there is a problem that methods that might be acceptable overseas could be applied to domestic operations and degrade the results. Some CSIS domestic counter-espionage operations do in fact utilize standard HUMINT techniques in order to gain intelligence and run agents, similar to MI5 operations in Britain and Northern Ireland. However, the greater problem rests with the aforementioned organizational culture of CSIS. The added strain of a foreign intelligence mandate abroad would add to the internal problems of CSIS and put even more strain on its relationship with the RCMP.

For such reasons, Western governments have typically maintained a separation between security and foreign intelligence collection. In contrast, centralized, repressive, and totalitarian governments have tended to combine the two functions within one agency. When a more or less democratic Russia emerged from the old USSR, for example, one of the first acts of the new government was to separate the two functions of the monolithic KGB (Hensler 2001). Official inquiries have generally recommended against expanding the CSIS foreign intelligence mandate. In 1981, for example, the MacDonald Commission noted the “danger of creating a security and intelligence monolith in a democratic state,” citing, “the dangers of contagion with respect to an espionage agency’s practice of violating the laws of other countries” (Canada 1981). In spite of its recommendations of 1990, three years later, SIRC suggested that a new foreign intelligence agency would be best located within the Privy Council Office or DFAIT (Hensler 2001). Martin Rudner testified before the Senate Committee on National Defence that, in his opinion, combining the different skills of specialized security and foreign intelligence capability is “not healthy ... lest too much power accumulate in too few hands” (Canada 2003a).

A later memorandum by the solicitor general suggests that the new resources and powers bestowed upon CSIS in the wake of 11 September, coupled with intense pressure to prevent further terrorist attacks, could compromise individual rights and have the potential for abuse by security intelligence agents (Bronskill 2002a). Generally speaking, Western intelligence operations maintain a firewall between security and foreign intelligence services that would be impossible to maintain if CSIS became Canada’s foreign intelligence agency. KGB is not a model to be emulated. The recent (2007) *Globe and Mail* editorial in favour of a single intelligence agency noted that the Netherlands and New Zealand model, which have combined foreign and security intelligence in a single administrative unit, ought to be followed by Canada. On geostrategic grounds alone – Holland has half the population of Canada and is smaller than Nova Scotia; New Zealand has been called a “dagger pointed at the heart of ... Antarctica” – such a suggestion is risible.

There are additional arguments against establishing a single agency with two possibly antithetical purposes. In its *2001 Annual Report*, SIRC indicated that because of the heavy workloads on

CSIS employees, important functions might not be handled expeditiously (Canada 2001d). For example, the average time taken by CSIS to process requests from Citizenship and Immigration Canada had risen significantly compared to previous years. During the period under review, SIRC noted that “the average time to process a case involving information briefs regarding high risk applicants was up to a year and a half.” Given the new priority of immigration screening since September 11, CSIS will continue to be fully occupied with security clearance requests and its domestic intelligence functions.

Counter-intelligence and counter-espionage functions should also be kept separate because CI methods often involve breaking local laws. Counter-espionage methods cannot do that. The first task of counter-intelligence is to assess the effectiveness of the adversary’s collection capabilities and targets. This knowledge indicates where one’s own information, communications, or activities are vulnerable and how best to protect them (Shulsky 1993). Counter-intelligence is essential to gain valuable information on foreign governments and to improve domestic security and intelligence programs. Without such foreign counter-intelligence, CSIS cannot be fully effective in its domestic operations. In the same way that the United States uses CIA to inform the FBI of foreign activities, a Canadian foreign intelligence agency would be required to inform CSIS and support its domestic security capability. This would allow CSIS to concentrate on domestic security and counter-espionage. A separate intelligence agency is required to avoid giving additional duties to an already overworked agency.

Funding for CSIS, beginning in 2001 and amounting to \$80M over two years in the 2007 budget, will undoubtedly assist the agency, but it does not address the systemic limitations that currently face the service. Recruiting and bureaucratic reform will take time anyway, and adding a foreign intelligence role would undermine the ability of CSIS to pursue its primary mandate and lead allied agencies constantly to question the intentions of the service. Every request made with respect to the security intelligence mandate of CSIS would be suspect, and information might be withheld to the detriment of Canada’s domestic security. CSIS is already working to capacity, already requires more resources, and is already fully occupied with its primary mandate: security intelligence. At present, CSIS simply could not house a foreign intelligence agency, even if it were deemed a good idea.

6 (b) A Canadian Foreign Intelligence Service – Where and Why?

Notwithstanding its traditional embrace of “soft power,” a new Canadian Foreign Intelligence Service, CFIS, will have to be located within DFAIT, the principal consumer of foreign intelligence. In much the same way as MI6 reports to the British foreign secretary and the Australian ASIS reports to the Australian minister of foreign affairs, the line of reporting for the director general of CFIS must be directly to the minister of foreign affairs. Within DFAIT there is considerable expertise concerning Canada’s international relations – foreign service, diplomatic staff, desk officers, and specialists in regional and national topics. DFAIT already receives shared American intelligence and directs foreign intelligence collection by CSIS and CSE through participation in various intelligence committees (Hensler 1995). In any case, close connections between Canadian foreign intelligence priorities and foreign policy objectives are needed, and direct reporting would ensure that it happened.

Increased interest in intelligence by DFAIT was most obvious following 11 September when then-foreign minister Manley announced that Canada’s intelligence capabilities were substandard and suggested establishing a separate foreign intelligence agency. In the aftermath of September 11, DFAIT pledged to increase its limited intelligence capability and undertake closer liaison with

the United States. In the *Canada-United States Smart Border Declaration*, the department pledged to “put the necessary tools and legislative framework in place to ensure that information and intelligence is shared in a timely and coherent way within our respective countries as well as between them” (Canada 2002f, online). DFAIT’s importance vis-à-vis foreign intelligence was underscored when John Manley was named chair of the Cabinet Committee on Public Security and Anti-Terrorism. Great interest in, and need for, intelligence exists within the department. Because it is key in targeting and utilizing foreign intelligence, DFAIT would be the most logical department to control CFIS.

Increased interest in intelligence can be seen elsewhere in the government as well, for the obvious reason that, in the post-9/11 security environment, only the willfully blind can ignore the need to gather intelligence regarding terrorists, peacekeeping missions, Canada’s commercial interests, and potential military deployments. Although many departmental intelligence consumers within the government would benefit from Canadian-supplied intelligence, the prime benefactors of such a new agency would be the executive. Under present circumstances, without a stream of accurate and independent raw data and an effective infrastructure to provide a finished product, the prime minister and the cabinet have become poor intelligence consumers. An improved capacity to collect and analyze foreign intelligence would allow analysts to create more accurate and timely estimates for the government. A high quality intelligence assessment with a strong cabinet minister responsible for insisting the product get to cabinet would allow more informed decision making on security and intelligence matters.

CFIS must not be an extension or adjunct of the Security and Intelligence Bureau of DFAIT, nor could it be. The bureau is tasked with intelligence gathering from open and diplomatic sources, and the other source of intelligence for DFAIT, the foreign and current intelligence divisions, provide analysis and assessment, also within DFAIT. To task these personnel with covert intelligence collection would be a mistake. Without the requisite training for clandestine operations, they would be woefully ill-equipped to handle such missions and would, in fact, be a liability. Additionally, since the bureau is already known in the international community as an open-source and analytical department within Canadian missions overseas, the sudden change in its mandate would precipitate corresponding changes in collection methods, thus betraying its new secret mission. Foreign officials would also become more circumspect about the type of information shared with Canadian diplomatic representatives. The analytical elements of DFAIT should remain in the department to provide open source, mission-specific analytical support for embassies and consulates.

In contrast, the new CFIS must operate under the official cover of ancillary mission staff, as do the intelligence operatives of other countries. As members of a Canadian mission abroad tasked with intelligence collection, CFIS agents would have access to DFAIT liaison personnel with first-hand knowledge of their target country and be eligible for diplomatic immunity as stipulated in the 1966 Vienna Convention on Diplomatic Relations (Kindred 2000). Sensitive budgetary matters relating to the operations of CFIS could also be concealed within the DFAIT budget in the same way that funding for the CSE is concealed within the DND budget.

The relationship between CFIS and CSE would be integral. In conjunction with CFIS, CSE would provide a general SIGINT-based picture and indicate where specific, on-the-ground investigation is needed. This would be undertaken by CFIS, eliminating reliance on American and British HUMINT. Similarly, CFIS would offer a method of verifying SIGINT received through CSE, and CSE would corroborate CFIS information, thus reducing the weakness of each source and multiplying its strengths. The process of selecting targets for CFIS would include consultation with CSE because it has experience targeting foreign intelligence collection. The key

agencies involved with selecting intelligence targets for CFIS would also include DFAIT, DND, the PMO, and a new, all-source analytic organization.

6 (b) i. Importance of Analysis

The funds required to create CFIS will be wasted unless a corresponding and robust analytic capability is developed. To remedy the problem of a weak analytic capacity, a new all-source and independent analysis organization should be created in the form suggested by Tony Campbell: a national intelligence analysis office (Campbell 2001). This new organization would be tasked with qualitative, quantitative, intellectual, and operational analysis from all sources. The concept of a separate analysis organization is not new: in the late 1960s, Starnes established an all-source operations room in External Affairs, and later, when he was director of CSIS, he recreated another in that organization. Both were modelled on a similar office in NATO (Starnes 1998, 127). In addition, the Macdonald Commission recommended the creation of such an agency. Moreover, the Office of National Assessments (ONA) is currently operating in Australia. In 1990, the SIRC report *In Flux But Not In Crisis* discussed ONA and its merits. They have not changed over the years.

The role of the Office of National Assessments is to produce analyses of international developments for the Australian prime minister and cabinet. It prepares reports, appreciations, and assessments on international political, strategic, and economic matters. ONA is not subject to external direction on the content of its assessments, and it is independent of any department or authority (Australia 2002). By reporting directly to the prime minister, however, ONA has access to politicians who are concerned with intelligence. It bases its assessments on information available to the Australian government from all sources, whether inside or outside the government, including open source material. ONA does not concern itself with domestic developments within Australia, does not collect intelligence by clandestine or other means, nor does it make recommendations for government policy; it is autonomous from any intelligence agency in Australia, and although the politicization of intelligence may be inevitable, its independence helps somewhat to remove analysis from operations and political influence (Friedman 2006; Ferris 2007).

Political influence is always a problem in intelligence analysis – as the British and American intelligence estimates regarding WMD in Iraq recently demonstrated. Generally speaking, intelligence is vulnerable to three political factors: pressures to adjust estimates to meet political objectives, opportunistic tendencies by analysts to do so, and the refusal by political masters to believe reports they feel are contrary to policy (Merom 1999). When not in accord with existing policy, intelligence is easily refuted or ignored. Removing an analytic cell from the oversight of an existing agency does not eliminate the possibility of politically coloured assessments, but it does tend to reduce the possibility. A Canadian ONA (CONA) could be established as an all-source, analytical cell on the Australian model. Based on input from CFIS, CSIS, CSE, DND, and DFAIT liaison personnel, CONA would produce short-term analysis as needed. Medium and long-range major intelligence and threat assessments to Canadian national security and a “priorities list” similar to the American National Intelligence Estimate (NIE) would also be produced to support the Interdepartmental Committee on Security and Intelligence. Unlike the existing Intelligence Assessment Secretariat which reports to the deputy clerk, CONA would report directly to another new creation, the Minister for Security and Intelligence, to whom the priorities list would be directed.

6 (b) ii. Focal Point for Canadian Intelligence

The intelligence role of the Privy Council would also require change. *In Flux But Not In Crisis* stated that SIRC was unable to assess whether the current system for coordinating, assessing, and disseminating intelligence was meeting Canadian security and intelligence needs (Canada 1990a). The Canadian intelligence community is decentralized and collegial, similar to the British community on which it is based. The collegial format has obvious defects: a propensity towards blandness and a search for the lowest common denominator in order to obtain agreement, as well as a tendency to search for solutions that obscure real differences and stitch departmental segments together instead of looking at subjects as a whole (Hermann 1996). Committee work creates an institutional pecking order and the oddities of group psychology. Despite the value of the interdepartmental group, good analysis at some point needs the clarity of a single mind working in depth without sectoral commitment and bias (Codevilla 1992; Friedman 2004). It seems to me that subtle and piecemeal reform to the existing intelligence community would only slightly improve matters and increase the already fragmented nature of departmentally driven intelligence machinery. Expanding the mandates of existing agencies would exacerbate, rather than solve, the problem of information diffusion. Agencies such as CSIS, CSE, and the Canadian Forces are already beset with problems of funding and overwork. Adding to their workload would probably prevent any new mandates, including foreign intelligence, from receiving their due, while simultaneously lowering the effectiveness of these organizations regarding primary tasks. Given the inefficiency within the existing Canadian intelligence infrastructure, expanding the roles of existing agencies would simply cause more problems.

Canadian intelligence is unfocused and divided. There is no single individual responsible for intelligence coordination such as the director of central intelligence in the United States or the chairman of the joint intelligence committee in Britain. A substantial centralizing reform to the Canadian intelligence infrastructure would not only provide independently collected intelligence, it would also provide guidance and direction to an otherwise amorphous and lethargic bureaucracy. There are enormous difficulties in the existing way that intelligence gets to cabinet and the prime minister, hence the need for a cabinet-level position, the minister for security and intelligence, who would be responsible for overseeing security and intelligence and ensuring that intelligence reaches the executive in a timely fashion.

In theory or on paper, the deputy clerk is currently mandated to coordinate the intelligence activities of the government; in fact, rarely is he or she held accountable because of the sheer volume of committee activity and the diffusion of authority within the Privy Council Office. According to the PCO itself, “no single cabinet minister is responsible for Canada’s security and intelligence community. Instead, a number of ministers are accountable for the activities of the organizations that report to each of them” (Canada 2001f, online). Consequently, the coordination of intelligence gathering, analysis, and threat assessment by the PCO – the apex of the civil service in Canada – reflects a ponderous management orientation rather than a strategic one. This would change. The intelligence assessment function would be removed entirely from the PCO and transferred to CONA. The new Ministry of Security and Intelligence would be the *de facto* focal point for Canadian intelligence activities, and any inquiries would be referred to the minister rather than the deputy clerk, who would no longer have an intelligence function. The Intelligence and Assessment Secretariat and the Security Intelligence Secretariat would both be moved to CONA and would provide the basis for the new analytical cell. Because CONA would give its priorities list directly to the minister, he or she would then have the requisite knowledge of intelligence operations and political accountability needed to act as the focal point for intelligence activities. The Intelligence Assessment Secretariat (IAS) would thus be chaired by the minister for security and intelligence. IAS would then become akin to the British Joint

Intelligence Committee, and it could discuss the implications of the priorities list derived from all-source collection and analysis. IAS would be restructured to reflect its new role and the model developed in the British government document, *National Intelligence Machinery*:

The main instrument for advising on priorities for intelligence gathering and for assessing its results is the Joint Intelligence Committee (JIC). It is a part of the Cabinet Office, under the authority of the Secretary of the Cabinet. It is responsible for providing Ministers and senior officials with regular intelligence assessments on a range of issues of immediate and long-term importance to national interests, primarily in the fields of security, defence and foreign affairs. The JIC also brings together the Agencies and their main customer Departments and officials from the Cabinet Office, to establish and prioritize the UK's intelligence requirements which are then subject to Ministerial approval. Intelligence on terrorism, the proliferation of weapons of mass destruction, and any other threats to the UK or to the integrity of British territory overseas are examples of high-priority requirements. (UK 2001)

To adapt this organizational model to Canada would require little more than changing the names, since both countries formally have parliamentary governments.

6 (b) iii. Accountability

To avoid the scandals that led to the elimination of the RCMP Security Service, parliamentary oversight is needed. Accountability is always a problem in bureaucracies. On the one hand, if accountability does not mean firings, it means nothing. On the other, intelligence analysis means risks, and some errors are inevitable. If supervisors hold their subordinates accountable, office politics become a factor, and thus intimidation and political infighting. This is why existing intelligence agencies in Canada have arms-length review organizations. But they also have separate ones as well: SIRC for CSIS and the Office of the Commissioner for the CSE. Presumably this separation of review mechanisms stems from the locations of these agencies in separate ministries, but the similarity of purpose – to provide scrutiny of the lawfulness of the activities of the two agencies – also creates duplication of effort. It would be extraneous to create yet another oversight committee, and better methods can be drawn from the British and Australian examples. In both countries, a review mechanism reporting directly to the prime minister is responsible for the review of intelligence activities.

In Australia, under article 29 of the Intelligence Services Act, the Parliamentary Joint Committee reviews the administration and expenditure of the entire Australian security and intelligence community, including their annual financial statements, and reports directly to Parliament (Australia 2001). In Britain, the Intelligence and Security Committee examines the expenditure, administration, and policies of the British intelligence community. It operates within the “ring of secrecy” and has wide access to the range of agency activities and to highly classified information (UK 2001). The committee is required to report annually to the prime minister on its work, and the committee's results are placed before Parliament for open discussion.

Canada could combine the review functions of SIRC, the CSE Commissioner, and the new CFIS review agency into one committee designed to oversee all Canadian intelligence activities. This committee would not be located within the Solicitor General or DND portfolios but would instead be an autonomous review committee located within the Privy Council Office and answerable directly to the prime minister, who in turn, would be required to report to Parliament. Not only

would such a committee eliminate the duplication of effort problems of having both a SIRC and a CSE commissioner, but it would help streamline the already excessively decentralized and politicized Canadian intelligence community.

6 (b) iv. Reforming Military Intelligence

As indicated above, the military intelligence infrastructure also needs reform. The Canadian Forces have long identified intelligence support as crucial for the success of peace support operations. The lack of intelligence planning doctrine during the African and former Yugoslavian operations has been addressed but not remedied. *Strategic Capability Planning for the Canadian Forces* (Canada 2000g) states that any Canadian military contribution will likely be led by the United States, emphasizing the need for interoperability with American forces while ignoring the need for Canada to develop independent intelligence doctrine. The United States will probably lead any future, traditional United Nations peacekeeping mission, and Canada is equally likely to participate. *The Joint Ops Planning Process Manual* assumes that the Canadian Forces will not be the lead country in a multilateral deployment. Consequently, it includes no doctrine or permanent mechanism for the challenges of being a lead nation (Hennessy 2001). Without a new doctrine to address these challenges, Canada will continue to rely on American intelligence for its military deployments, and these will not necessarily be available.

JTF-2, which deployed to Afghanistan in December 2001, needed real-time operational and strategic intelligence support for their missions. While CIA supports American Special Forces and MI6 supports the British Special Air Service, there is no corresponding support for JTF-2. Like most of Canada's military-intelligence community, JTF-2 relies on its allies for strategic intelligence. If Canada is to be an effective member of a multilateral deployment, whether the United States is the lead nation or not, a new doctrine must be created, including national information operation protocols and liaison between other Canadian intelligence assets and Canadian special forces.

Canadian Forces Information Operations (CFIO) was issued under the direction of the 1997 Defence Planning Guidance. The CFIO doctrine acknowledges that information operations must be integrated in a government-wide strategy in support of political and military objectives (Bourque 2001). Bourque noted that intelligence support is critical to the planning, execution, and assessment of information operations – it must support the intelligence preparation of the battle space by identifying threats and providing offensive or defensive measures against them. This doctrinal change to defence intelligence must include liaisons between military intelligence formations and other government agencies. Interaction and coordination at the ministerial level could occur in the proposed and reformed Interdepartmental Committee for Security and Intelligence and would help ensure the coordination of Canada's defence and foreign intelligence. CONA would greatly improve defence intelligence because it would provide analysis as needed to DND. Canadian Forces liaison members would have immediate access to political and strategic intelligence prior to deployment as well as ongoing support throughout the mission through defence attaches or CFIS liaison personnel. Thus, CONA would improve defence intelligence by providing current intelligence to the Canadian Forces, but also by coordinating intelligence from other Canadian sources to assist future deployments.

7. CONCLUSION

Canada would benefit from a dedicated foreign intelligence agency and analytic community. Without the ability to monitor, identify, and engage potential threats overseas, Canada will be forced to rely on its allies, follow a reactive security policy, and remain a soft target for espionage and terrorist activity. As the nature of North American security changes, Canada needs a better intelligence system to support Canadian or continental defence operations. The system within which Canadian intelligence operated during the Cold War has changed. While Canada was able to function effectively in the UKUSA or NORAD alliances because of its geographical proximity to the former USSR, the value of its location declined drastically with the end of the Cold War. During this time, Canada has relied on the United States to provide finished intelligence and allowed its own collection and analysis capabilities to atrophy. International security has evolved significantly since September 11. Canadian intelligence must now operate in a new strategic environment for which its traditional methods are poorly suited.

Canada must be able to verify intelligence from its allies, to make informed foreign policy decisions (such as whether to take part in a military action in Iraq), and to avoid being dis-informed intentionally or inadvertently. Foreign intelligence will also be critical for counter-intelligence operations directed at detecting hostile activities abroad, including terrorism. Terrorists are often well aware of communications security protocols and, because of the nature of their activities, are highly skilled at maintaining operational security in their attacks. Most of the time, the only way to obtain effective intelligence on terrorist groups will be through an independent, foreign HUMINT program. Defence intelligence will also be important as Canada becomes more involved militarily with the United States in the war on terrorism and in multilateral operations. Canada will have to develop a foreign HUMINT capacity to overcome the gap between commitment and credibility that led to intelligence disasters in Africa and the former Yugoslavia. Without an independent foreign intelligence capability, Canada will continue to receive the foreign intelligence its allies want it to have, with potentially devastating political and economic implications. The Privy Council Office acknowledged that the Canadian security and intelligence community is a key asset in the government's efforts to protect Canada and Canadians, and that "government has a responsibility to monitor threats to Canada so it can take action" (Canada 2001f, online). Unless it develops a foreign HUMINT capability, Canada will not be able to meet that responsibility.

Among the benefits of a Canadian foreign intelligence service would be a reduced reliance on shared American intelligence. Creating a finished product designed specifically for Canadian consumption and cast in Canadian policy terms would necessarily improve the way government uses intelligence. This would also help to avoid an erosion of sovereignty as Canada moves toward a coordinated North American defence command and a more active role in joint military deployments. It would also address the persistent issue of Canada's worthiness as an ally –stated negatively, it would address the issue of Canada as a free-rider with respect to defence and security policy. Canada can no longer rely on signals intercepts of Soviet communications as its chief alliance contribution. CFIS would provide new information to share with allies and help maintain Canada's limited alliance influence. It is critical to stay at the allied table. If Canada were to leave or be asked to leave, it would never have access to such information again.

The creation of a more centralized intelligence infrastructure that included CFIS and CONA analysis would better coordinate the intelligence cycle. Existing agencies could concentrate on their primary mandates and benefit from the new intelligence provided by CFIS and CONA. A new authority for intelligence activities and a new dedicated cabinet position would help ensure that assessments were accurate, timely, and available to departmental consumers and to cabinet.

The fluid nature of international security post-9/11 is reason enough to be clear about the need for CFIS and CONA. The point of CFIS is not to create an agency that might engage in such Cold War activities as overthrowing governments or undertaking political assassinations like some mid-twentieth-century junior KGB or CIA. Rather it is a question of streamlining and making Canada's information intelligence bureaucracy effective. At the very least, it is necessary to revisit the 1993 *SIRC Counter-Intelligence Study* because of the altered circumstances of international politics today and the changing nature of current threats.

In the past, Canada based its foreign policy on its status as a middle power and its reputation as an international arbiter. With the Canadian military contribution in Afghanistan and increasingly coordinated continental security, Canada may well move towards a more integrated defence and security relationship with the United States. Canada has already been declared an al-Qa'ida target, and al-Qa'ida affiliates and other terrorist groups operate in the country. A closer relationship with the United States will no doubt make Canada a more prominent target, not just for terrorist networks but for state-based espionage as well. In any comprehensive foreign and military policy review, a reconsideration of the position of security and foreign intelligence must play an important part.

An accurate, responsive, and comprehensive intelligence capability is a fundamental cornerstone of Canada's sovereignty. It alone can provide the national situational awareness necessary for the development of coherent and informed security policy. The inadequacies of Canada's intelligence community have been well known to specialists since the end of World War Two. The terrorist attack on the United States brought these same deficiencies to the attention of a wider public, including the Canadian political leadership. Fixing the intelligence deficit has become an obvious imperative, and creating a Canadian Foreign Intelligence Service can play a major part in future Canadian security policy.

Note: The views expressed in this publication are those of the author and not CDFAI.

BIBLIOGRAPHY ³

- Aldrich, Richard A. 2002. Dangerous Liaisons: Post–September 11 Intelligence Alliances. *Harvard International Review* 24, no. 2: 50–54.
- Andrew, Christopher. 1991. The British View of Security and Intelligence. In *Security and Intelligence in a Changing World: New Perspectives for the 1990s*, ed. S. Farson, D. Stafford, and W. Wark, 127–48. London: Frank Cass.
- . 1994. The Making of the Anglo-American SIGINT Alliance. In *The Name of Intelligence: Essays in Honor of Walter Pforzheimer*, ed. H.B. Peake and S. Halpern, 95–109. Washington: NIBC Press.
- Australia. Joint Intelligence Committee. 1954. *Cooperation in British Commonwealth Defence*. National Archives, series A5954169, barcode: 464680 (1954–1956) [accessed 02/05/2004].
- . 2001. *Intelligence Services Act 2001*. Canberra: HMSO.
- . 2002. Office of National Assessments, home page. Available at: <<http://www.ona.gov.au>> [accessed 28/01/2002].
- Baker, Stewart. 1994. Should Cops be Spies? *Foreign Policy* 97 (Winter): 36–53.
- Bamford, James. 2002. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*. New York: Anchor.
- Barber, Cdr Josh. 2001. An Intelligence, Surveillance and Reconnaissance (ISR) Vision for the Canadian Forces. *Canadian Military Journal* 2, no. 4: 41–46.
- BBC News Online. 2002. US Ready to Go it Alone, 2 February. Available at: <http://news.bbc.co.uk/1/hi/english/world/europe/newsid_1798132> [accessed 01/02/2004].
- Beare, Margaret E. 2003. Policing with a National Security Agenda, *Canadian Heritage*, February. Available at: <<http://www.canadianheritage.gc.ca/progs/multi/pubs/police/security-e.cfm>> [accessed 30/10/2004].
- Beaumont, Peter, and David Rose. 2002. MI6: We Now Need Twice as Many Spies. *The Observer*. Available at: <<http://www.observer.co.uk/waronterrorism/story/0,1373,665031,00.html>> [accessed 17/03/2002].
- Bell, Stewart. 2002a. Canada on Terrorists' Hit List, Officials Say. *National Post*. Available at: <<http://www.nationalpost.com/search/story.html?f=/stories/20011215/877751.html&q=isis>> [accessed 26/01/2002].
- . 2002b. Axis Harbours Nuclear Plans: CSIS. *National Post*, A6, 26 February.
- . 2003. CSIS Admits to Spying Abroad: First Public Confirmation. *National Post*, A1, 20 October.
- . 2004. *Cold Terror: How Canada Nurtures and Exports Terrorism Around the World*. Toronto: Wiley.
- . 2005. "Big League" Spying Needed, Ottawa Told. *National Post*, A6, 19 May.
- . 2006. Listening in on the Enemy, *National Post*. A1, 15 April.
- . 2007. Canada Listening in on Taliban Exchanges. *National Post*, A1, 1 May.
- Bendetto, Richard. 2004. Data Sought on Secret Spending. *USA Today*, 2 February. Available at: <http://www.usatoday.com/news/washington/2004-02-02-secret-spending_x.htm> [accessed 07/02/2004].
- Bercuson, David. 1996. *Significant Incident: Canada's Army, the Airborne, and the Murder in Somalia*. Toronto: McClelland & Stewart.

³ Many of the online sources cited have been taken off the Internet since they were accessed for this paper. We regret that we are unable to provide up-to-date online sources for some of the documents cited.

- Black, Eldon. 1996. *Direct Intervention: Canada–France Relations, 1967–1974*. Ottawa: Carleton University Press.
- Blackwell, Tom. 2002. Immigration Canada Seeks Consultant to Clear Backlog. *National Post*, A9, 25 January.
- Blanchfield, Mike. 2002. Cellucci Suggests We Buy Our Own Planes. *National Post*. Available at: <<http://www.nationalpost.com/news/story.html?f=/stories/20020220/110469.html>> [accessed 21/02/2002].
- Bothwell, Robert. 1998. The Cold War and the Curate's Egg: When Did Canada's Cold War Really Begin? *International Journal* 53, no. 3: 407–18.
- Bourque, J. D. R. 2001. *Information Operations for Canada*. Available at: <<http://www.cfsc.dnd.ca/irc/amsc/amsc1/003.html>> [accessed 04/08/2001].
- Bronskill, Jim. 1999. Lost Document Among Four Recent Leaks Plaguing CSIS. *The Edmonton Journal*, A6, 16 November.
- . 2001a. Canada at Risk of Growing Terrorism. *Calgary Herald*, A13, 13 June.
- . 2001b. PM Outside Intelligence Loop. *Calgary Herald*, A6, 4 October.
- . 2002. CSIS Watchdog Warns of Potential for Abuse. *National Post*, A7, 22 January.
- . 2004. Canadian Spies Mounting More Overseas Operations to Counter Terror Threat. *CNEWS*, 1 June. Available at: <<http://circ.jmellon.com/docs/html>> [accessed 15/09/2004].
- . 2005. Secret Spy Agency's Staff, Budget Raised. *The Globe and Mail*, 13 June. Available at: <<http://www.theglobeandmail.com/servlet/story/LAC.20050613.SPY.13/BNPrint/theglobeandmail/Canada>> [accessed 13/06/2005].
- Brown, Jim. 2001. Foreign Spy Agency Eyed. *CNEWS*. Available at: <http://www.canoe.ca/CNEWS/Attack011005/05_spy-cp.html> [accessed 05/10/2001].
- . 2002. Terrorist Crisis Revives Debate on Foreign Spy Agency for Canada. *Canadian Press*. Available at: <<http://www.recorder.ca/cp/national/011014/n101436A.html>> [accessed 18/02/2002].
- Campbell, Anthony. 2001a. Opening Remarks of Speech, CASIS Conference, Dalhousie University, Halifax, 28 September.
- . 2001b. Canada–United States Intelligence Relations and “Information Sovereignty.” In *Canada Among the Nations, 2003: Coping with the American Colossus*, ed. D. Carment, F. O. Hampson, and N. Hillman, 79–103. Toronto: Oxford University Press.
- Canada. 1946. *Royal Commission on Espionage Report*. Ottawa.
- . House of Commons. 1969. *Debates*, 10636–38, 26 June. Ottawa.
- . 1981. *Commission of Inquiry Concerning Certain Activities of the RCMP: Freedom and Security under the Law*. 2nd report, vol. 1. Ottawa.
- . Security Intelligence Review Committee. 1987. *Annual Report 1986–1987*. Ottawa.
- . Security Intelligence Review Committee, Peter Russell. 1988. *Should Canada Establish a Foreign Intelligence Agency?* Ottawa.
- . House of Commons. 1990a. *In Flux but Not in Crisis: A Report of the House of Commons Special Committee on the Review of the CSIS Act and the Security Offences Act*. Ottawa.
- . Security Intelligence Review Committee. 1990b. *Annual Report*. Ottawa.
- . Security Intelligence Review Committee. 1995. *Counter-Intelligence Study 93-06*, January 1994; expurgated version, July.

- Canada. Office of the Auditor General. 1996a. *The Canadian Intelligence Community: Control and Accountability*. Available at: <<http://www.oagbvg.gc.ca/domino/reports.nsf/alb15d892a1f761a852565c40068a492/4f626474cefb11f5852565d90072f17e?OpenDocument&Highlight=0,intelligence>> [accessed 22/01/2002].
- . Department of National Defence (DND), Army Lessons Learned Centre. 1996b. Training for Operations. *Dispatches* 3, no. 1.
- . Canadian Security Intelligence Service (CSIS). 1996c. *Canadian Security Intelligence Service Public Report*. Available at: <http://www.csis-scrs.gc.ca/eng/publicrp/pub1996_e.html> [accessed 23/01/2002].
- . CSIS. 1997a. *Canadian Security Intelligence Service Public Report*. Available at: <http://www.csis-scrs.gc.ca/eng/publicrp/pub1997_e.html> [accessed 23/01/2002].
- . DND, Army Lessons Learned Centre. 1997b. *Analysis Report*. Ottawa.
- . 1997c. *Report of the Somalia Commission of Inquiry*. Available at: <<http://www.forces.gc.ca/somalia/somaliae.htm>> [accessed 07/08/2006].
- . CSIS. 1998a. *Canadian Security Intelligence Service Public Report*. Available at: <http://www.csis-scrs.gc.ca/eng/publicrp/pub1998_e.html> [accessed 22/01/2002].
- . DND, Army Lessons Learned Centre. 1998b. *Intelligence Support – Operations in the Former Yugoslavia*. Ottawa.
- . CSIS. 1999a. *Canadian Security Intelligence Service Public Report*. Available at: <http://www.csis-scrs.gc.ca/eng/publicrp/pub1999_e.html> [accessed 23/01/2002].
- . Special Senate Committee on Security and Intelligence. 1999b. *Report*. Available at: <<http://www.parl.gc.ca/36/1/parlbus/commbus/senate/com-e/secu-e/rep-e/repsecintjan99part1-e.htm>> [accessed 23/01/2002].
- . Security Intelligence Review Committee. 2000a. *Annual Report 1999–2000*. Ottawa.
- . Department of Foreign Affairs and International Trade (DFAIT). 2000b. *Audit of Security*. Ottawa.
- . DND. 2000c. *Strategic Capability Planning for the Canadian Forces*. Ottawa.
- . 2000d. *Canadian Security Intelligence Service Public Report*. Available at: <http://www.csis-scrs.gc.ca/eng/publicrp/pub2000_e.html#4a> [accessed 23/01/2002].
- . 2000e. *Canadian Security Intelligence Service Report #2000/04 – International Terrorism: The Threat to Canada*. Available at: <http://www.csis-scrs.gc.ca/eng/miscdocs/200004_e.html> [accessed 22/01/2002].
- . 2000f. *Canadian Security Intelligence Service Perspectives #2000/01 – Trends in Terrorism*. Available at: <http://www.csis-scrs.gc.ca/eng/miscdocs/200001_e.html> [accessed 23/01/2002].
- . DND, Vice Chief of Defence Staff. 2000g. *Strategic Capability Planning for the Canadian Forces*. Ottawa.
- . DND, Vice Chief of Defence Staff. 2000h. *The Intelligence Analyst's Handbook*. Ottawa.
- . DND. 2000i. *History of the 1st Canadian Division Intelligence Company (1989–2000)*. Available at: <<http://www.dnd.ca/menu/operations/CFJOG/html/IntCoy-e.htm>> [accessed 22/06/2004].
- . CSIS. 2001a. *Special Allocation of Funds to Security and Intelligence Organizations*. News release. Available at: <http://www.csis-scrs.gc.ca/eng/press/press20011019_e.html> [accessed 26/01/2002].
- . CSIS. 2001b. *Economic Espionage: Clandestine Methods Used to Disadvantage Canadian Interests*. Available at: <http://www.csis-scrs.gc.ca/eng/aware/aware3_e.html> [accessed 11/03/2002].
- . Canadian Space Agency (CSA). 2001c. *Canada's International Business Strategy*. Available at: <<http://www.space.gc.ca/business/ibd/cibs/strategic.asp>> [accessed 14/03/2002].

- Canada. Security Intelligence Review Committee. 2001d. *Report 2000–2001: An Operational Audit of CSIS*. Ottawa.
- . Security Intelligence Review Committee. 2001e. *The CSIS Act*. Available at: <<http://www.sirc-csars.gc.ca/5000.html>> [accessed 07/08/2006].
- . Privy Council Office. 2001f. *Canadian Security and Intelligence Community*. Available at: <http://www.pco-bcp.ca/default.asp?Language=E&Page=publications&doc=si/si_toc_e.htm> [accessed 23/09/2004].
- . DND. 2001g. *HUMINT During Peace Support Operations*. *Dispatches* 8, no. 1.
- . DND. 2001h. *Report of the Somalia Commission of Inquiry*. Available at: <<http://www.dnd.ca/somalia/vol3/v3c25ce.htm>> [accessed 09/08/2005].
- . DND. 2002a. *History of 1st Canadian Division Intelligence Company (1989–2000)*. Available at: <http://www.dnd.ca/menu/Operations/CFJOG/html/IntCoy_e.htm> [accessed 21/01/2002].
- . DFAIT. 2002b. Key Objectives of Canada's Foreign Policy. From *Canada in the World: Canadian Foreign Policy Review (1995)*. Available at: <<http://www.dfait-maeci.gc.ca/dfait/mandate-e.asp>> [accessed 06/02/2005].
- . DFAIT. 2002c. *Sources of Federal Government Information, 1999–2000*. Available at: <<http://www.dfait-maeci.gc.ca/dfait/infosource-chap46-e.asp>> [accessed 21/01/2006].
- . DFAIT, CanadExport On-Line. 2002d. *Market Research Centre Key to Unlocking Foreign Markets*. Available at: <<http://circ.jmellon.com/docs/view.asp?id=123>> [accessed 08/10/2007].
- . DFAIT. 2002e. *Canada's Anti-Terrorism Plan*. Available at: <<http://www.dfait-maeci.gc.ca/anti-terrorism/anti-terrorism-e.asp>> [accessed 13/03/2004].
- . DFAIT. 2002f. *Terrorism and the US–Canada Border*. Available at: <<http://www.dfait-maeci.gc.ca/can-am/content/sec110-7-e.asp>> [accessed 14/03/2004].
- . DFAIT. 2002g. *The Canada–US Smart Border Declaration*. Available at: <<http://www.dfait-maeci.gc.ca/anti-terrorism/declaration-e.asp>> [accessed 14/03/2002].
- . Department of the Solicitor General. 2002h. *Overview of the Department of the Solicitor General*. Available at: <<http://www.sgc.gc.ca/eoverview.htm>> [accessed 27/01/2002].
- . CSIS, Samuel Porteous. 2002i. *Economic/Commercial Interests and Intelligence Services*, Commentary #59/1995. Available at: <http://www.csis-scrs.gc.ca/eng/comment/com59_e.html> [accessed 23/01/2003].
- . Security Intelligence Review Committee. 2002j. *Annual Report*. Ottawa.
- . Standing Committee on National Defence and Veterans' Affairs, May. 2002k. *Facing Our Responsibilities: The State of Readiness of the Canadian Forces*. Report. Ottawa.
- . Standing Senate Committee on National Security and Defence. 2003a. *Evidence*. Ottawa. Available at: <http://www.parl.gc.ca/37/2/parlbus/commbus/senate/Com-e/defe-e/10evb-e.htm?Language=E&Parl=37&Ses=2&comm_id=76> [accessed 04/02/2003].
- . House of Commons, Subcommittee on National Security of the Standing Committee on Justice and Human Rights. 2003b. *Evidence*. 2nd session, 37th Parliament. Ottawa. Available at: <<http://www.cmte.parl.gc.ca/cmte/CommitteePublication.aspx?SourceID=61457&PARLSES=3728&JNT=0&COM=3298>> [accessed 01/04/2005].
- . House of Commons, Hansard. 2003c. Bill C-409, *An Act to Establish the Canadian Foreign Intelligence Agency*. Ottawa. Available at: <<http://www2.parl.gc.ca/HouseBills/BillsPrivate.aspx?Language=E&Mode=1&Parl=37&Ses=2#C409>> [accessed 17/03/2003].
- . DND. 2003d. *Joint Intelligence Doctrine*, B-GJ-005-200/FP-000. Ottawa.

- Canada. Privy Council Office. 2004a. *Securing an Open Society: Canada's National Security Policy*. Available at: <http://www.pco-bcp.gc.ca/docs/Publications/NatSecurnat/natsecurnat_e.pdf> [accessed 10/02/2005].
- . CSIS. 2004b. *Public Report 2003*. Ottawa.
- . Standing Senate Committee on National Security and Defence. 2005a. *Unrevised Evidence*. 15 January. Ottawa [accessed 18/03/2006].
- . Special Senate Committee on the Anti-Terrorism Act. 2005b. *Evidence*. 15 March. Available at: <<http://www.parl.gc.ca/38/1/parlbus/commbus/senate/com-e/05eva.e.htm>> Ottawa [accessed 14/03/2007].
- . DND, Canadian Defence Academy. 2007. *Leadership in the Canadian Forces*. Ottawa.
- CASIS. 2002. *CASIS Newsletter #39*. Ottawa: Canadian Association of Security and Intelligence Studies.
- . 2007. Annual Conference. Calgary, AB.
- Chwialkowska, Luiza. 2001. It's Time We Dirtied Our Hands, Say Spy Agency Proponents: Terrorism Prompts Renewed Calls for Canadian Foreign Intelligence Agency, *National Post Online*. Available at: <<http://www.canada.com/news/story.asp?id={7656EE62-4F3F-4244-9572-3C32198ADDA5}>> [accessed 03/11/2001].
- Cleroux, Richard. 1989a. *Official Secrets: The Story Behind the Canadian Security Intelligence Service*. Toronto: McGraw-Hill Ryerson.
- . 1989b. Limited Overseas Use of CSIS Agents Urged. *The Globe and Mail*, A3, 28 September.
- CNN. 2002. Americans, Canadians Evacuated from Jakarta. Available at: <<http://www.cnn.com/WORLD/asiapcf/9805/15/Indonesia>> [accessed 22/01/2004].
- Codevilla, Angelo. 1992. *Informing Statecraft: Intelligence for a New Century*. New York: Free Press.
- Cohen, Andrew. 2003. *While Canada Slept: How We Lost Our Place in the World*. Toronto: McClelland & Stewart.
- Communications Security Establishment. 2002. *CSE's Place in Government*. Available at: <http://www.cse.dnd.ca/en/about_cse/about_cse.html> [accessed 21/01/2003].
- Cooper, Barry. 2002. Canadian Discourse on Peacekeeping. In *International Intervention: Sovereignty versus Responsibility*, ed. M. Keren and D. A. Sylvan, 126–46. London: Frank Cass.
- . 2004a. The Sadism of Moralizing Canadian Multilateralism. In *Independence in an Age of Empire: Assessing Unilateralism and Multilateralism*, ed. G. F. Walker, 284–92. Halifax: Centre for Foreign Policy Studies.
- . 2004b. *New Political Religions, or an Analysis of Modern Terrorism*. Columbia: University of Missouri Press.
- Cooper, Barry, Mercedes Stephenson, and Ray Szeto. 2004. *Canada's Military Posture: An Analysis of Recent Civilian Reports*. Vancouver: Fraser Institute.
- Cordesman, Anthony. 2001. *Beyond Bosnia: The Need for Realism in Using American Military Force*. Available at: <http://www.csis.org/component/option,com_csis_pubs/task,view/id,1577> [accessed 31/10/2003].
- Canadian Press (CP). 2004. Panel Ponders CIA-style Spy Service for Canada. [accessed 15/09/2004].
- Dallaire, Romeo. 2004. *Shake Hands with the Devil: The Failure of Humanity in Rwanda*. Toronto: Vintage.
- Daly, Brian. 2001. FBI Requests More Money to Increase Canadian Presence. *National Post*, A12, 17 December.
- Donnelly, John. 2002. Aspects Familiar to Some. *The Boston Globe*. Available at: <http://www.boston.com/news/packages/underattack/globe_stories/0912/Aspects_familiar_to_some+.shtml> [accessed 17/01/2002].

- Dorn, A. Walter. 1999. The Cloak and the Blue Beret: The Limits of Intelligence-Gathering in UN Peacekeeping. *Pearson Papers Number 4: Intelligence in Peacekeeping*. Clementsport, NS: Lester B. Pearson Canadian International Peacekeeping Centre.
- . 2005. Intelligence at UN Headquarters? The Information and Research Unit and the Intervention in Eastern Zaïre, 1996. *Intelligence and National Security* 20, no. 3: 440–65.
- Duffy, Andrew. 2001. US Trial Judge Slams “Canadian Way.” *Calgary Herald*, A12, 28 March.
- Eayrs, James. 1965. *In Defence of Canada: Vol. 2 – Appeasement and Rearmament*. Toronto: University of Toronto Press.
- Elcock, Ward. 2002a. *Submission to the Special Committee of the Senate on Security and Intelligence*. Available at: <http://www.csis-scrs.gc.ca/eng/miscdocs/kelly_e.html> [accessed 26/01/2003].
- . 2002b. Talking points for lecture at Carleton University, 12 June. Ottawa: CSIS. Available at: <<http://www.csis-scrs.gc.ca>> [accessed 12/04/2003].
- Elliot, S. R. 1981. *Scarlet to Green: A History of Intelligence in the Canadian Army 1903–1963*. Toronto: Canadian Intelligence and Security Association.
- Farson, A. Stuart. 1997. In Crisis and In Flux?: Politics, Parliament and Canada’s Intelligence Policy. *Journal of Conflict Studies* 16, no. 1. Available at: <<http://www.lib.unb.ca/Texts/JCS/bin/get.cgi?directory=s96/articles/&filename=farson.html>> [accessed 15/09/2004].
- Farson, Stuart. 1993. Accountable and Prepared: Reorganizing Canada’s Intelligence Community for the 21st Century. *Canadian Foreign Policy* 1, no. 3: 28–37.
- . 1999. Is Canadian Intelligence Being Reinvented? *Canadian Foreign Policy* 6, no. 2: 1–17.
- FAS. 2002. *Canadian Intelligence Agencies*. Available at: <<http://fas.org/irp/world/canada/cse/index.html>> [accessed 21/01/2004].
- Ferris, John. 2007. Intelligence Reform and the Primacy of Politics. *Dispatch* 5, no. 1. Available at: <<http://www.cdfai.org/newsletters/newslettersspring2007.htm>> [accessed 10/04/2007].
- Finn, Thomas D’Arcy. 1993. Does Canada Need a Foreign Intelligence Service? *Canadian Foreign Policy* 1, no. 3: 149–62.
- Flynn, Michael. 2001. Guilty Until Proven Innocent. *Bulletin of the Atomic Scientists* 57, no. 2: 14–17.
- Foulkes, Charles. 1945. Memo for COS and N. A. Robertson. 22 DEC 45 HQ file 22-1-43, vol. 1, RG 24, vol. 6178.
- Franks, C. E. S. 1983–84. Parliamentary Control of Securities Activities. *McGill Law Journal* 29: 326–39.
- Freeze, Colin. 2006. Spy Chief Reveals Extent of Foreign Missions. *The Globe and Mail*, A1, 28 October.
- . 2007. Canada Called Easy Target for Spies. *The Globe and Mail*, A6, 6 June.
- Friedman, George. 2006. The Intelligence Problem. *Stratfor*, 9 May. Available at: <<http://www.stratfor.com>> [accessed 05/09/2006].
- Frost, David, and Michael Gratton. 1994. *Spyworld: Inside the Canadian and American Intelligence Establishments*. Toronto: Doubleday.
- Furuhovde, Maj-gen Trond. 1995. Organization and Planning Requirements: Lessons Drawn from Past Ops. From *Improving the Prospects for Future International Peace Operations*, Workshop Proceedings. Washington, DC: US Government Printing Office.
- Galloway, Gloria. 2007. No New Agency for Foreign Intelligence, Top Spy Says. *The Globe and Mail*, 29 May. Available at: <<http://www.theglobeandmail.com/servlet/story/RTGAM.20070529.wsecurity29/BNstory/National/home>> [accessed 29/05/2007].
- Gibbons, Jim. 2002. Protecting America: The HUMINT Challenge. *The Hill*. Available at: <http://www.hillnews.com/092601/ss_gibbons.shtm> [accessed 13/03/2005].

- Gladwell, Malcolm. 2005. *Blink: The Power of Thinking Without Thinking*. New York: Little, Brown and Co.
- Globe and Mail*. 2007. Not Another Spy Agency. Editorial, A12, 6 June.
- Godfrey, Tom. 2004. Critics: RCMP, CSIS Cuts Threaten Security. *The Toronto Sun*, A12, 28 October.
- Goldenberg, Eddie. 2006. *The Way It Works: Inside Ottawa*. Toronto: McClelland & Stewart.
- Goodspeed, Peter. 2000. The New Space Invaders: Spies in the Sky. *National Post*, 19 February. Available at: <<http://www.fas.org/irp/program/process/docs/000219-echelon.htm>> [accessed 06/11/2004].
- Gordon, James. 2004. Security Experts Back Foreign Spy Agency. *National Post*, A4, 30 January.
- Graham, Patrick. 2001. Aid Group Accused of Taking Sides. *National Post*, A1, 3 February.
- Granatstein, J. L. 1981. *A Man of Influence: Norman A. Robertson and Canadian Statecraft*. Ottawa: Deneau.
- . 1988. *The Ottawa Men: The Civil Service Mandarins, 1935–1957*. 2d ed. Toronto: University of Toronto Press.
- . 2002. *Canada's Army: Waging War and Keeping the Peace*. Toronto: University of Toronto Press.
- Granatstein, J. L., and David Stafford. 1990. *Spy Wars: Espionage and Canada from Gouzenko to Glastnost*. Toronto: Key Porter.
- Granatstein, J. L., and Robert Bothwell, eds. 1982. *The Gouzenko Transcripts: The Evidence Presented to the Kellock–Taschereau Royal Commission of 1946*. Ottawa: Deneau.
- Great Britain. 2002. *Intelligence and Security Committee Annual Report 1999–2000*. Available at: <http://www.official-documents.co.uk/cgi-bin/htm_hl?DB=off-docsl&STEMMER=en&WORDS=intellig+&COLOUR=Red&STYLE=s&URL=http://www.archive.officialdocuments.co.uk/document/cm48/4897/4897-02.htm#muscat_highlighter_first_match> [accessed 26/01/2004].
- Ha, Tu Thanh. 2001. Judge Says CSIS Agents Must Testify. *The Globe and Mail*, A10, 2 February.
- Hager, Nicky. 1996. *Secret Power: New Zealand's Role in the International Spy Network*. Nelson: Craig Potton.
- . 1998. Exposing the Global Surveillance System. *Covert Action Quarterly*. Available at: <<http://www.jya.com/echelon.htm>> [accessed 06/11/2004].
- Handel, Michael. 1989. *War, Strategy, and Intelligence*. London: Frank Cass.
- Handel, Michael, and John Ferris. 1995. Clausewitz, Intelligence, Uncertainty and the Art of Command in Military Operations. *Intelligence and National Security* 10, no. 1: 1–58.
- Hennessy, Michael. 2001. Operation Assurance: Planning a Multi-National Force for Rwanda/Zaire. *Canadian Military Journal* 2, no. 1: 11–20.
- Hensler, Alistair. 1995. Creating a Canadian Foreign Intelligence Service. *Canadian Foreign Policy* 3, no. 3. Available at: <<http://www.carleton.ca/cfpj/issue-archive-3.3.html#hensler>> [accessed 17/03/2007].
- . 1999. Canadian Intelligence: An Insider's Opinion. *Canadian Foreign Policy* 6, no. 3. Available at: <<http://www.carleton.ca/cfpj/issue-archive-6.3.html#hensler>> [accessed 17/03/2007].
- . 2001. CSIS Has No Business in Foreign Intelligence. *Ottawa Citizen*, A4, 29 October.
- Hermann, Michael. 1996. *Intelligence Power in Peace and War*. Cambridge: Cambridge University Press.
- Hulnick, Arthur. 1997. Intelligence and Law Enforcement: The “Spies are not Cops” Problem. *International Journal of Intelligence and Counterintelligence* 10, no. 3: 213–31.
- Humphreys, Adrian. 2002. RCMP Boosts its Presence Overseas. *National Post*, A4, 27 March.
- Johnson, Loch. 1996. *Secret Agencies: US Intelligence in a Hostile World*. New Haven: Yale University Press.
- Johnston, Dale. 1997. No Cloak and Dagger Required: Intelligence Support to UN Peacekeeping. *Intelligence and National Security* 12, no. 4: 348–61.
- Kaplan, Robert. 2002. *Warrior Politics: Why Leadership Demands a Pagan Ethos*. New York: Ballantine.

- Kasurak, Peter. 2003. *Accountability for Intelligence in Peacekeeping Operations: Canada's Operation Assurance as a Case Study*. Available at: <<http://www.carleton.ca/csds/pk/pki/pki-conference2003.htm>> [accessed 20/07/2007].
- Kealey, Greg. 1993. The Early Years of State Surveillance of Labour and the Left in Canada: The Institutional Framework of the RCMP Security and Intelligence Apparatus, 1918–26. *Intelligence and National Security* 8, no. 3: 127–41.
- Kealey, Greg, and Reg Whitaker. 1993. *RCMP Bulletins – The Depression Years, 1933–34*. St. John's: Canadian Committee on Labour History.
- Keegan, John. 2003. *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda*. Toronto: Key Porter.
- Keeley, James. 2000. Organizing the United Nations for Commercial Satellite Imagery. Paper presented at The Need to Know: The Use of Commercial Satellite Imagery and Canadian Security Needs Conference, 17–18 November, Calgary.
- . 2004. The Use of Commercial Satellite Images and Canadian Security Needs. In *Commercial Satellite Imagery and United Nations Peacekeeping*, ed. J. F. Keeley and R. Huebert, 87–98. Burlington: Ashgate.
- Kennedy, Kristan. 2006. *Canada and the Intelligence-Gathering Burden: Should Ottawa Spy Abroad?* Royal United Services Institution for Defence and Security Studies, Transatlantic Relations Program, 24 November. Available at: <<http://www.rusi.org/research/studies/transatlantic/commentary/ref:C456710449A93D>> [accessed 01/12/2006].
- Kindred, Hugh, et al. 2000. *International Law: Chiefly as Interpreted and Applied in Canada*. Document Supplement. Toronto: Emond Montgomery.
- Knight, Amy. 2005. *How the Cold War Began: The Gouzenko Affair and the Hunt for Soviet Spies*. Toronto: McClelland & Stewart.
- Law Union Brief to the Parliamentary Committee Reviewing the CSIS Legislation. 1990. In *SIRC – The Review of the CSIS Act and the Security Offences Act*. #31 (15 May): 31A–8. Appendix CSIS-6.
- Levin, Duncan. 2002. The CIA and the Price We Pay: Lawsuit Response Puts the Figure at \$26.6 Billion. *The Baltimore Sun*. Available at: <<http://www.gwu.edu/~cnss/secret/dloped.html>> [accessed 26/01/2004].
- Littleton, James. 1986. *Target Nation: Canada and the Western Intelligence Network*. Toronto: Lester and Orpen Dennys.
- Livesey, Bruce. 1998. Trolling for Secrets: Economic Espionage is the New Niche for Government Spies. *InfoWar*. Available online [accessed 22/01/2003].
- Ljunggren, David. 2002. Canada Freezes Idea for Intelligence Agency. *National Post*, A1, 11 April.
- Lynn-Philip, Hodgson. 2002. *Inside Camp X*. 3rd ed. Port Perry: Blake Books.
- MacCharles, Tonda. 2004. PM Wants to Expand Overseas Spy Service: Martin's View Pleases Expert. *The Toronto Star*, 7 February. Available at: <<http://circ.jmellon.com/docs/html>> [accessed 15/09/2004].
- Mayeda, Andrew. 2006a. RCMP, CSIS Sign Peace Accord. *Calgary Herald*, A6, 27 October.
- . 2006b. CSIS Bosses Frustrate MPs. *Calgary Herald*, A5, 1 November.
- . 2007a. Intelligence “Czar” Needed, Former CSIS Director Says. *National Post*, A8, 27 March.
- . 2007b. Conservatives' Foreign Spy Agency Promise in Limbo. *Ottawa Citizen*, 13 February. Available at: <<http://www.canada.com/ottawacitizen/news/story.html?id=2d5c45b6-c071-4c38-a669-e87123a47639&k=86973>> [accessed 13/02/2007].
- . 2007c. Ottawa May Still Boost Canada's Foreign Intelligence. *Ottawa Citizen*, 30 April. Available at: <<http://www.canada.com>> [accessed 5/1/2007].

- Mayeda, Andrew. 2007d. Tories Drop Plan to Build Foreign Spy Agency. *Ottawa Citizen*, 16 May. Available at: <<http://www.canada.com>> [accessed 5/16/2007].
- McClintock, Maria. 2004. *Canada Eyes Spies Abroad*. Available at: <http://circ.jmellon.com/docs/html/canada_eyes_spies_abroad.html> [accessed 28/04/2005].
- Mellon, Jerome. 2001. *The UKUSA Agreement of 1948*. Available at: <<http://cv.jmellon.com/papers.html>> [accessed 15/10/2004].
- Merom, Gil. 1999. The 1962 Cuban Intelligence Estimate: A Methodological Perspective. *Intelligence and National Security* 14, no. 3.
- Mintz, John. 2001. Unseen Perils in a Russian Squall. *The Washington Post*, A1, 3 January.
- Mofina, Rick. 2001. CSIS Boss Given Wider Range of Power. *Calgary Herald*, A10, 3 November.
- Morden, Reid. 2003. Spies, Not Soothsayers: Canadian Intelligence in the 21st Century, *CSIS Commentary*, 85.
- . 2006. A Canadian Foreign Intelligence Service: A New Necessity or an Expensive Frill? *CDFAI*. Available at: <<http://www.cdfai.org/outreach.htm>> [accessed 14/03/2007].
- Mount, Graeme. 1993. *Canada's Enemies: Spies and Spying in the Peaceable Kingdom*. Toronto: Dundurn.
- Naime, Doug, and Bruce Owen. 1993. Secret War Waged to Stay Alive. *Winnipeg Free Press*, B3, 21 December.
- NATO. 2006. NATO Standardization Agency, Glossary of Terms and Definitions (AAP-6). Available at: <<http://www.nato.int/docu/stanag/aap2006/AAP-6-2006.pdf>> [accessed 15/03/2007].
- Nickerson, Colin. 1999. Spy Blunder Draws Criticism in Canada. *The Boston Globe*, A4, 18 November.
- Noel-Baker, Francis. 1955. *The Spy Web*. New York: Vanguard.
- Off, Carol. 2000. *The Lion, the Fox and the Eagle: A Story of Generals and Justice in Yugoslavia and Rwanda*. Toronto: Random House.
- O'Neill, Juliet, and Matthew Fisher. 2007. Canadian Link in Alleged Spy Operations. *National Post*, A3, 5 February.
- Parkinson, Ted. 2006. Has the Time Arrived for a Canadian Foreign Intelligence Service? *Canadian Military Journal* (Summer). Available at: <<http://www.journal.forces.gc.ca/engraph/Vol7/No2/PDF/05-Parkinson-e.pdf>> [accessed 17/03/2007].
- Pratt, David. 2003. *Does Canada Need a Foreign Intelligence Agency?* Available at: <<http://www.davidpratt.net>> [accessed 02/02/2004].
- Priest, Dana. 2003. *The Mission: Waging War and Keeping Peace with America's Military*. New York: Norton.
- Pugliese, David. 2001. Budget Cuts Hurt our Ability to Spy, Forces Chiefs Say. *National Post Online*. Available at: <<http://www.nationalpost.com/news/national/story.html?f=/stories/20010616/593730.html>> [accessed 06/16/2001].
- Quiggin, Thomas. 1995. Response to "No Cloak and Dagger: Intelligence Support to UN Peacekeeping." *Intelligence and National Security* 13, no. 4: 385–401.
- Ramsbotham, Gen Sir David. 1995. Peace Reinforcement Organizational Planning and Technical Requirements. In *Improving the Prospects for Future International Peace Operations*. US Congress, Office of Technology Assessment, Workshop Proceedings. Washington: US Government Printing Office.
- Ratcliff, R.A. 2006. *Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers*. Cambridge: Cambridge University Press.
- Richelson, Jeffrey. 1993. *The US Intelligence Community*. Boulder: Westview.
- Richelson, Jeffrey, and Desmond Ball. 1990. *The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries*. Boston: Allen and Unwin.

- Robinson, Bill. 2002. *An Unofficial Look Inside the Communications Security Establishment, Canada's Signals Intelligence Agency*. Available at: <<http://watserv1.uwaterloo.ca/~brobinso/cse.html>> [accessed 21/01/2003].
- Rosen, Philip. 2000. *The Canadian Security Intelligence Service*. Ottawa: Parliamentary Research Branch, Library of Parliament, Current Issue Review 84–27E.
- Ross, Jen. 2002. CSIS Does Have Spies Abroad, *PoliticsWatch*. Available at: <[http://politicswatch.com/10-18-01\(2\).htm](http://politicswatch.com/10-18-01(2).htm)> [accessed 14/01/2003].
- Rudner, Martin. 2000. *Canada's Communications Security Establishment: From Cold War to Globalization*. Ottawa: NPSIA.
- . 2001. Canada's Communications Security Establishment from Cold War to Globalization. *Intelligence and National Security* 16: 97–128.
- Sallot, Jeff. 1996. To Spy or Not to Spy? *The Globe and Mail*, A1, 2 September.
- Sawatsky, John. 1980. *Men in the Shadow: The RCMP Security Service*. Toronto: Doubleday.
- Sears, Val. 2004. Canada Must Use Its Spies, *Canoe.ca*, 20 July. <<http://circ.jmellon.com/docs/html>> [accessed 07/08/2006].
- Senior, Hereward. 1991. *The Last Invasion of Canada: The Fenian Raids, 1866–1870*. Toronto: Dundurn.
- Sevunts, Levon. 2000. Foreign Intelligence Agencies Busy in Our Business. *The Gazette*, 23 July. Available at: <<http://www.securityfocus.com/archive/12/73289>> [accessed 08/02/2005].
- Shulsky, Abram. 1993. *Silent Warfare: Understanding the World of Intelligence*. Washington: Brassey's.
- Smith, Hugh. 1994. Intelligence and UN Peacekeeping. *Survival* 36, no. 3: 85–96.
- Sokolsky, Joel. 1989. A Seat at the Table: Canada and its Alliances. *Armed Forces and Society* 16, no. 1: 11–35.
- Solicitor General. 2002. New Technologies, Intelligence Sharing and Integrated Law Enforcement to Improve Safety and Security of Canadians. Available at: <<http://www.sgc.gc.ca/Releases/e20011012.htm>> [accessed 26/01/2004].
- Spector, Norman. 2002. We Must Help Root Out Evil. *The Globe and Mail*, A14, 14 February.
- Stafford, David. 1986. *Camp X: Canada's School for Secret Agents, 1941–45*. Toronto: Lester and Orpen.
- Stairs, Denis, et al. 2003. *In the National Interest: Canadian Foreign Policy in an Insecure World*. Calgary: CDFAI.
- Starnes, John. 1982. When Spying Spells Chaos. *Macleans*, 16 August: 9.
- . 1987. A Canadian Secret Intelligence Service? *International Perspectives* (July/Aug).
- . 1992. Espionage Canada? *Ottawa Citizen*, A11, 2 July.
- . 1998. *Closely Guarded: A Life in Canadian Security and Intelligence*. Toronto: University of Toronto Press.
- Stephenson, William. 1977. *A Man Called INTREPID: The Secret War, the Authentic Account of the Most Decisive Intelligence Operations of World War II*. Toronto: Ballantine.
- . 1999. *British Security Coordination: The Secret History of British Intelligence in the Americas, 1940–1945*. New York: Fromm International.
- Sudoplatov, Pavel, and Anatoli Sudoplatov. 1994. *Special Tasks: The Memoirs of an Unwanted Witness – A Soviet Spymaster*. New York: Little, Brown and Co.
- Thompson, John C., and Joe Turlej. 2003. *Other People's Wars: A Review of Overseas Terrorism in Canada*. Toronto: Mackenzie Institute.
- Travers, James. 2004. Foreign Spy Service Would Pose Problems: Fine-Tuning CSIS Would Be a Better Solution. *The Toronto Star*, 6 March. Available at: <<http://circ.jmellon.com/docs/html>> [accessed 15/09/2004].

- Trickey, Mike. 2001. Spy Defector Flees to US, Russian Embassy Admits, *National Post*, 19 March. Available at: <<http://www.nationalpost.com/news/national/story.html?f=/stories/20010317/503463.html>> [accessed 26/08/2003].
- UK Stationary Office. 2001. *National Intelligence Machinery*. Available at: <<http://www.archive.official-documents.co.uk/document/caboff/nim/0114301808.pdf>> [accessed 1/09/2007].
- United States. 2004. *The 9/11 Commission Report*. New York: Norton.
- Wark, Wesley. 1989. The Evolution of Military Intelligence in Canada. *Armed Forces and Society* 16, no. 1: 77–98.

CANADIAN DEFENCE & FOREIGN AFFAIRS INSTITUTE

CDFAI is the only think tank focused on Canada's international engagement in all its forms - diplomacy, the military, aid, and trade security. Established in 2001, CDFAI's vision is for Canada to have a respected, influential voice in the international arena based on a comprehensive foreign policy, which expresses our national interests, political and social values, military capabilities, economic strength, and willingness to be engaged with action that is timely and credible.

CDFAI was created to address the ongoing discrepancy between what Canadians need to know about Canadian international activities and what they do know. Historically, Canadians tend to think of foreign policy – if they think of it at all – as a matter of trade and markets. They are unaware of the importance of Canada engaging diplomatically, militarily, and with international aid in the ongoing struggle to maintain a world that is friendly to the free flow of goods, services, people, and ideas across borders and the spread of human rights. They are largely unaware of the connection between a prosperous and free Canada and a world of globalization and liberal internationalism.

In all its activities, CDFAI is a charitable, nonpartisan organization, supported financially by the contributions of foundations, corporations and individuals. Conclusions or opinions expressed in CDFAI publications and programs are those of the authors and speakers and do not necessarily reflect the views of the Institute staff, fellows, directors, advisors, or any individuals or organizations that provide financial support to CDFAI.

