TOP SECRET

File No.: 2800-173
(TD R526)

CSIS'S COLLABORATION WITH COMMUNICATIONS SECURITY ESTABLISHMENT CANADA (CSEC)

(SIRC STUDY 2012-05)

Security Intelligence Review Committee
March 6, 2013

TABLE OF CONTENTS

1 INTRODUCTION 3

2 METHODOLOGY AND SCOPE 4

3 UNDERSTANDING CSEC 5
- 3.1 CSEC Mandate 5
- 3.2 The Merging of SIGINT and HUMINT 6
- 3.3 Cooperation at a Glance 7
- 3.4 Overseas Operations 8

4 ONGOING CHALLENGES TO THE CSIS/CSEC RELATIONSHIP 10
- 4.1 The Limits of Shared Services 10
- 4.2 Knowledge Transfer and Joint Risk Management 11
- 4.3 The s.16 Program 12
- 4.4 Information Sharing 13

5 RESPONSIBILITY FOR CYBER SECURITY 16
- 5.1 Key Challenges 16
- 5.3 Moving Forward 19

6 CONCLUSION 20

1 INTRODUCTION

The relationship between CSIS and the Communications Security Establishment Canada (CSEC) has changed dramatically over the past half decade. Although they once functioned principally as two solitudes within the Canadian intelligence domain, rising government demands for s.12 and s.16 information have compelled CSIS and CSEC to increase the coordination of their intelligence collection strategies and processes. This review explores the benefits to CSIS from its increased cooperation with CSEC, through an examination of operational and non-operational initiatives.

The review starts with an overview of CSEC's mandate, and the unique attributes of the international alliance of which CSEC is a member. The review then looks at the state of cooperation between CSIS and CSEC,
As has been increasingly the case among Canada's allies, the world of signals intelligence and the world of human intelligence have been drawn closer together in order to keep up with changing threats and to maximize intelligence efficiency. Overall, the Committee was impressed by the intelligence benefits to CSIS of closer cooperation with CSEC, and agrees that closer cooperation is both desirable and valuable.

The review then turns to some of the challenges encountered with increasing cooperation. These include: coordinating corporate services; ensuring sufficient inter-organizational knowledge transfer; managing operational risks;
and, the adequacy of direction and policies used to help guide CSIS's information sharing with CSEC.

The final section of the review identifies an anomaly of the relationship; namely, a noted lack of cooperation on cyber security. The study ends with a recommendation encouraging CSIS to develop stronger overarching principles of cooperation with CSEC.

2 METHODOLOGY AND SCOPE

This review examined the recent evolution of CSIS's relationship with CSEC. SIRC looked at changes in the arrangements and the policies governing the partnership, as well as information-sharing practices and procedures. In particular, SIRC assessed a sample of joint CSIS-CSEC operational initiatives to provide insight into how they have enhanced CSIS's collection activities, and examined a wide assortment of corporate documentation to help contextualize the unprecedented cooperation between these partners.

SIRC also attended several briefings with working-level employees and senior-level executives, and had the opportunity to speak to a CSEC employee working at the Service as part of the secondment program.

The core review period ran from January 1, 2011 to March 31, 2012, although some information from outside the period was taken into consideration to broaden an understanding of important issues.

3 UNDERSTANDING CSEC

CSEC is the main provider of foreign intelligence to the Canadian Government. Arising from the cryptographic developments of World War II,[1] CSEC was formally established in 1946 as the 'Communications Branch' within Canada's National Research Council, receiving its current name in 1975 after it was transferred to the National Defence portfolio. The Government of Canada publicly acknowledged CSEC's existence in 1983, although it was not until Canada's involvement in Afghanistan that CSEC garnered sustained public attention.[2]

3.1 CSEC Mandate

CSEC collects, analyses and reports on signals intelligence (SIGINT), a term given to information gathered by intercepting and studying radio, wire, radar, telecommunications and other electronic transmissions.[3] CSEC's responsibilities derive from three mandates:

A) To acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
B) To provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and,
C) To provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.[4]

Under Canadian law, CSEC's activities are not to be directed against Canadians or any person in Canada. However, when collecting SIGINT under Mandate A, CSEC may incidentally acquire personal information about Canadians. This information may be retained if assessed as essential to understanding the foreign intelligence, and it may be included in reporting shared with CSIS, so long as it is minimized.[5] Activities under

[1] The term cryptography is the science of protecting information by encrypting it. This science accelerated during W.W.II with the emergence of professional agencies devoted to code-making (cryptography) and code-breaking (cryptanalysis).

[2] On November 16, 2011, CSEC was established as a stand-alone agency. This administrative change made the Chief of CSEC a Deputy Head and Accounting Officer, with responsibility to report directly to the Minister of National Defence. Prior to this change, the Chief reported to the National Security Advisor, Privy Council Office, on policy and operational issues, and to the Deputy Minister of Defence on administrative and financial matters. No mandate changes resulted from this new designation, and CSEC remained within the National Defence portfolio.

[3] SIGINT comprises, either individually or in combination, communications intelligence (COMINT), electronics intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT). Refer to "Canadian SIGINT Security Standards," CSIS Cooperation with CSEC File 520-47, Vol.3

[4] *National Defence Act*, s.273.64, (1), last amended on March 6, 2012.

[5] Information that is 'minimized' obscures the names of Canadians or Canadian entities.

Mandate C (Support to Lawful Access) require that CSEC act as an agent of the department or agency requesting assistance; however, CSEC does not retain the information.

CSEC participates in international collaboration and information exchanges as part of a special SIGINT arrangement with the United States' National Security Agency (NSA), the United Kingdom's Government Communications Headquarters (GCHQ), Australia's Defence Signals Directorate (DSD) and New Zealand's Government Communications Security Bureau (GCSB). The collection methods used by this alliance are highly sensitive,

3.2 The Merging of SIGINT and HUMINT

SIGINT and human intelligence (HUMINT) agencies have long been regarded by intelligence professionals as generally occupying mutually exclusive, albeit complementary roles. CSIS, which relies on HUMINT, has security intelligence as its primary mandate; it has also a limited mandate to collect foreign intelligence, and may collect this information only *within* Canada. CSEC – a SIGINT agency – has foreign intelligence as its primary mandate, and may not direct its activities at Canadians or any person within Canada. For almost two decades, therefore, these intelligence agencies operated largely in isolation from each another.

Before passage of the *Anti-Terrorism Act* in 2001, the *Criminal Code* prohibited CSEC from intercepting any communication that originated or terminated in Canada, and where the originator had an expectation of privacy. Since 2001, however, CSEC may intercept one-end Canadian communications, subject to strict conditions, for purposes of either obtaining foreign intelligence or of protecting Government computer systems or networks.[6] This new authority has moved CSEC increasingly into areas once dominated by CSIS,[7]

[6] Two new collection authorities were granted to CSEC: the first enables CSEC to collect the communications of foreign intelligence targets even if those communications go into or out of Canada. The overriding condition for the collection of such private communications is that the interception must be directed at foreign entities abroad. The second new authority enables CSEC to intercept private communications in the course of assisting the Government in safeguarding its computer systems and networks. Refer to "CSEC's Ministerial Authorizations: New Authorities," CSEC Website.

[7] "The Anti-Terrorism Act and CSEC's Evolution," CSEC Website.

In 2007, CSIS and CSEC co-authored a letter to the Clerk of the Privy Council describing the unique opportunities for the Government in physically locating CSEC HQ alongside CSIS HQ. Soon thereafter, a joint working group was created to explore what increased collaboration would mean to both organizations, albeit within existing legislative parameters.

3.3 Cooperation at a Glance

The efforts begun in 2007 have paid dividends, moving the relationship from sporadic engagement to daily collaboration. There is high-level involvement (i.e. CSIS Director and Chief of CSEC), and a new Memorandum of Understanding which outlines arrangements for cooperation on collection, sharing and operational support. Emblematic of this cooperation was the revamping of the CSIS/CSEC secondment program in 2011. Although secondments were not new, from CSIS's perspective it was apparent that secondees were acting principally as emissaries, as opposed to genuine employees. Therefore, the new program made secondees full-fledged employees, with all the access and responsibilities of their colleagues, again paralleling secondment practices between the

There is also daily contact between CSIS and CSEC at multiple working levels, across all operational branches. Owing to the Service's experience in managing these relationships in order to execute

CSIS and CSEC also routinely participate in international forums alongside allied agencies. Whether the issue is cyber attacks by foreign governments, or the evolution of espionage using technological means, the consensus among allied partners is that the strict boundaries once drawn between HUMINT and SIGINT are less and less distinct.

3.4 Overseas Operations

Despite the challenges discussed in the following sections of this review, the Committee was impressed by the intelligence benefits to CSIS of closer cooperation with CSEC. Indeed, SIRC believes that it is in Canada's national security interests for this evolving partnership to further coalesce, albeit within the practical limitations prescribed by the respective mandates of each organization.

4 ONGOING CHALLENGES TO THE CSIS/CSEC RELATIONSHIP

4.1 The Limits of Shared Services

As noted earlier, the 2007 letter to the Clerk of the Privy Council highlighted a number of benefits of locating CSEC HQ alongside CSIS HQ. Chief among these were cost savings from mutual cooperation between (at that time) largely segregated agencies. This optimism was reiterated by the National Security Advisor a few years later, who affirmed that collaboration was more important than ever within the security and intelligence community. It was widely believed, therefore, that once CSIS and CSEC were working side-by-side, communication would become easier, resulting in effective operational synergies.[13]

The focal point of this collaboration was a strategy of 'shared services' – i.e. facilities management and/or corporate support functions that can be performed by CSIS and shared with CSEC, or *vice versa*. For intelligence agencies faced with increasingly limited resources in a period of Government-wide fiscal constraints, shared services lend themselves to efficient and effective resource management. Unfortunately, **SIRC found that the initial expectations for shared services between CSEC and CSIS may have been too optimistic.**

To a significant extent, the high expectations have been offset by managerial issues, budgetary restrictions, and complications related to CSEC-site development. The challenges range from salary differences, complications in standardizing health, safety and employment regulations and certifications, to managing differences between the employment criteria for CSEC's unionized versus CSIS's non-unionized employees.

The new CSEC HQ remains under construction; at this time, it

[13] CSIS Briefing Note, "Proposed New Governance Model for CSEC-CSIS Collaboration on Shared Enabling Services," File 370-625, October 1, 2010; and, CSIS Document, "A Vision for the Future – A White Paper," File 370-625, October 1, 2010; and, Joint Management Meeting, "CSIS and CSEC – Record of Discussion," December 11, 2009.

appears that the initial cost-savings touted in 2007, and repeatedly embraced as one of the key reasons justifying co-location, will not be as significant as initially projected.[15]

4.2 Knowledge Transfer and Joint-Risk Management

Difficulties in negotiating shared services are relatively easy when compared to efforts to increase the integration of CSIS and CSEC collection, which entail altogether different organizational perspectives and methodologies related to the collection, retention, analysis and dissemination of information. Indeed, **SIRC found that gaps in understanding the other organization's respective mandate and/or responsibilities were a recurring theme.** This issue was raised at both the working and managerial levels across CSIS's operational branches, and acknowledged at joint-CSIS/CSEC meetings, as an impediment to cooperation.

One area given considerable attention by both agencies is risk management.

[15] SIRC Meeting with CSIS Assistant Director Technology (ADT), June 19, 2012; and, "CSIS/CSEC Shared Services Proposed Governance Model Meeting – Record of Discussion," File 370-625, January 27, 2011.

4.3 The s.16 Program

Previous SIRC reviews have raised the concern that CSIS's collection of s.16 information could negatively impact the Service's primary mandate to collect security intelligence.

4.4 Information Sharing

SIRC found, however, that a significant risk of increased SIGINT-HUMINT collaboration is the potential erosion of control over the information.

Normally, the Service exercises control over the use of information via either caveats and/or assurances: CSIS caveats stipulate that the information being provided is CSIS property, and cannot be forwarded to another agency or altered without CSIS's direct consent. Assurances are formal, bilateral agreements made with foreign agencies stipulating that CSIS's information will not be used in a manner which runs contrary to international human rights conventions. The extent to which caveats and/or assurances are effective depends on the degree of trust between CSIS and the agency receiving the information.

CSIS's caveats and assurances, however, were never designed for SIGINT collection.

HUMINT-to-SIGINT information exchanges are low risk endeavours. This is premised on the fact that allied agencies are primarily focussed on their own national intelligence priorities. However, of concern to SIRC are those instances when allied collection

priorities have coalesced with Canada's – such as in counter-terrorism cases.

It is clear to SIRC that both Ministerial Direction and associated CSIS policies are designed to prevent the misuse/abuse of information, both from a security and human rights perspective. However, it is not clear how CSIS can comply with Ministerial Direction stipulating that caveats must be used when sharing information with domestic and foreign recipients, when SIGINT collection and dissemination functions run contrary to this expectation.[35]

For its part, CSIS has acknowledged that addressing concerns on this complex subject "remains a work in progress".[36] Considering that CSIS/CSEC collaboration is expected to increase, SIRC will revisit this issue in subsequent reviews in order to assess what progress has been made in addressing this challenge.

[36] Refer to ER&L Email to SIRC, "FWD: SIRC Study – CSIS Relationship with CSEC," October 15, 2012.

5 RESPONSIBILITY FOR CYBER SECURITY

Over the past four years, CSIS has steadily received direction from government

5.1 Key Challenges

5.3 Moving Forward

In 2010, Public Safety Canada created a whole-of-government Cyber Strategy which asserts that there can be no ambiguity in terms of who does what. The Strategy confirms the respective roles of CSEC and CSIS: the former has the recognized expertise in dealing with cyber threats and attacks, while the latter is broadly tasked to analyze and investigate domestic and international threats. The Strategy notwithstanding, **SIRC's review found that there is still work to be done to coordinate CSIS' cyber-related activities with CSEC, especially with respect to the protection of information infrastructure of importance to the Government of Canada.**

Canada needs an effective system for managing cyber threats, both by ensuring a strong capability to investigate cyber-espionage, and by maintaining robust cyber-defence and mitigation systems. **Given the inevitability of growth in CSIS/CSEC collaboration as well as their impending collocation, we would strongly encourage CSIS to develop clearer and more robust overarching principles of cooperation with CSEC. These principles should address the growing volume of challenges which have arisen between the two agencies, while respecting the individual mandates of each organization.**

6 CONCLUSION

Indeed, after reviewing CSIS's files and speaking to a number of employees, SIRC believes that it is in Canada's national security interests for this evolving partnership to continue towards increased levels of collaboration. However, this must be done in accordance with the respective mandates of each organization.

Although SIRC is in contact with the CSEC Commissioner's office, there is no authority for our offices to engage in cooperative review. We believe this should be of concern to both the Minister of Public Safety and the Minister of National Defence, each of whom must rely on two separate review processes to provide (incomplete) insight into the integrated activities of their respective intelligence agencies.