TOP SECRET

File No.: 2800-159
(TD R510)

CSIS'S INVESTIGATION CYBER THREAT

(SIRC STUDY 2010-07)

Security Intelligence Review Committee
June 23, 2011

TABLE OF CONTENTS

1 INTRODUCTION

Canada has long been a target of foreign espionage activities because of its scientific and technological capacity, Recently, the Director of CSIS stated that Canada is experiencing levels of espionage comparable to the height of the Cold War,[1] some performed through the use of information operations or "cyber attacks". Not surprisingly, cyber threats, have become a new priority for the Government of Canada. Accordingly, CSIS has been directed to provide

In fall 2010, the Government introduced *Canada's Cyber Security Strategy*. This whole-of-government strategy defines the roles and responsibilities of federal departments and agencies on a range of cyber issues, including cyber-espionage. Given its expertise and mandate, Canada's signals intelligence agency,[3] the Communications Security Establishment Canada (CSEC) plays a key role. The strategy calls on CSEC to enhance its capacity to detect and discover threats, and to respond to cyber threats and attacks against government communications networks and information technology systems.

In order to fulfill its own mandate, which is echoed in the *Strategy*, CSIS has developed a two-pronged approach

1 Refer to CBC documentary on CSIS - interview with Brian Stewart, April 22, 2010.

3 Signals Intelligence, or SIGINT, consists of information obtained from intercepted communications, radars, or data transmissions.

This review examines CSIS's investigation of the cyber threat posed and more broadly, how CSIS's efforts contribute to Canada's cyber security. First, we examine the threat, as well as some of the key challenges associated with its investigation. We then take a closer look at the strategies and tools CSIS is using to move the investigation forward, CSIS's revamped approach to cyber threat is establishing clear benchmarks to assess the future success of the investigation. Finally, we explore CSIS's role within a broader "whole of government" approach to countering the cyber threat. This discussion suggests that as CSIS positions itself in the future, it should remain guided by the investigative role assigned to it by government and statute.

2 METHODOLOGY AND SCOPE

For this review, SIRC examined and CSIS policy. SIRC also examined documents related to the creation and implementation of *Canada's Cyber Security Strategy*, as well as the Service's cooperation with other federal government departments, private Canadian industry, and the research community. In addition, SIRC was privy to several briefings by the

The time period of this review ran from January 1, 2007 to August 31, 2010, although were taken into account to broaden an understanding of key issues.

3 CYBER ESPIONAGE THREAT

3.1 Cyber-Attacks: A Newer Version of Traditional Counter-Espionage

In the past decade, espionage threat has expanded into the cyber realm because of greater technical expertise and capacity. At its core, however, cyber-espionage is merely a newer means to achieve the same ends as 'traditional' espionage: the collection of information by one state on another. In addition, cyber-espionage also focuses on countering

The advantages of cyber-espionage over traditional espionage include: the low cost in comparison to training and mobilizing human spies; the ability to target weak links in a large network, and, the difficulty of identifying specific cyber-attackers

5 CSIS'S ROLE IN CANADA'S CYBER SECURITY STRATEGY

In fall 2010, the Government released *Canada's Cyber Security Strategy* to tackle criminal and security threats emanating from the cyber realm. The document sets out three key goals: first, to create a comprehensive, centralized approach to dealing with cyber threats; second, to outline the role of specific federal departments and agencies in countering those threats, and; third, to support and reinforce existing structures involved in the cyber file."[22]

The strategy emphasizes the importance of domestic partnerships on cyber issues.[23] From CSIS's perspective, the relationship with CSEC is particularly crucial since CSEC is the agency responsible for protecting the Government's computer systems and networks, and for providing it with related mitigation advice.

---

22 The *Strategy* also emphasizes shoring up existing structures aimed at combating cyber threats, such as the Canadian Cyber Incident Response Centre (CCIRC), Canada's "focal point for cyber incident response".

23 The RCMP is to investigate "suspected domestic and international crime acts against Canadian networks and information infrastructure." *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*. Government of Canada, 2010.

5.1 Issue for Consideration

In accordance with its mandate, and as outlined in the *Strategy,* CSIS's role is to "analyze and investigate" domestic and international cyber threats to the security of Canada; CSIS is therefore one of many players that supports wider Government efforts

Mitigation, which refers to advice provided to victims, or potential victims, from designated government agencies, does not fall within CSIS's mandate on this file.

However, **as CSIS positions itself to keep pace with the threat, it should remain focused on its investigative role, and continue to use caution not to engage in activities that could be seen as mitigation**.

6 CONCLUSION

By examining the nature of the cyber threat and the strategies and tools developed by the Service, this review outlines some of the challenges and opportunities related to the investigation. In addition, the review examines the ongoing limits of the Service's role in a "whole of government" strategy –