TOP SECRET

File No.: 2800-156
(TD R507)

CSIS'S OPERATIONAL USE OF THE INTERNET

(SIRC STUDY 2010-04)

Security Intelligence Review Committee
May 3, 2011

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In recent years, Internet activities have moved to the forefront of a number of national security investigations. This review explores the existing strategies, policies and processes which guide CSIS's operational use of the Internet

The review found the Internet to be a valuable investigative tool for CSIS. The Service's approach to investigative activities involving the Internet, both in terms of policy and procedure, is sound with ample flexibility required to adapt to the Internet's rapidly evolving nature. SIRC identified two considerations for CSIS when using the Internet for operational purposes.

The first consideration relates to youth. Almost all youth spend time on the Internet they are also often targets for extremist Internet propaganda. As a result, the likelihood of CSIS coming into possession of information dealing with minors in the course of its investigations has increased. Ministerial Direction and internal CSIS direction have already stressed the need for CSIS to give special consideration when dealing with youth. CSIS should therefore impress upon its employees the need to exercise added caution when collecting and retaining information relating to a youth.

The second consideration relates to open source information. Although a great deal of open source information can be collected from the Internet, SIRC wishes to remind CSIS employees that such information should still be subject to the same "strictly necessary" test as information received from other sources.

1 INTRODUCTION

In the span of a decade, the Internet has gone from being a simple mail delivery system and repository of information to a far more interactive medium, allowing users to create and share content, to communicate and participate in ways that previously had not been possible. The result of this transformation has been both positive and negative. Positively, the Internet has become an investigative tool for CSIS; for example, key targets of the Toronto 18 were initially detected through the Internet. At the same time, however, there are negative implications, such as enabling people who may have never met each other to create networks, mobilize and plan potential threat-related activities without ever having to leave their home. As a result, Internet activities are at the forefront of a number of recent national security investigations.

Of concern to national security is the growing contribution the Internet has on the radicalization of individuals, both in Canada and abroad, who may become threats to Canadian interests.[2]

The Internet plays an important role at every stage of radicalization, giving direct access to unfiltered extremist ideology, as well as providing an anonymous virtual meeting place for like-minded radical individuals. It also offers opportunities to build relationships and gain expertise and skills that were previously only provided in overseas training camps, thus giving potential terrorists easy access to operational information to help plan and execute a terrorist attack.[3]

This review sought to explore the existing strategies, policies and processes which guide CSIS's operational use of the Internet. It examines a number of questions, such as: what kind of information can be obtained from the Internet that cannot be obtained

[2] CSIS defines radicalization as " the process of moving from moderate beliefs to extremist beliefs. Muslim radicalization is the process of moving from moderate, mainstream Islamic beliefs to a belief that violence can legitimately be used to support and promote a fundamental view of Islam" from, CSIS Study 2006-7/09(b), "The Radicalizers: The Islamist Extremism Threat to Canada from Within" (April 16, 2007), p. 3.

[3] "Violent Islamic Extremism, the Internet, and the Homegrown Terrorist Threat", Majority and Minority Staff Report, May 8, 2008, p 3.

through conventional means? What additional operational value does the collection of open information obtained on the Internet provide to CSIS investigations? What are some of the difficulties of using the Internet as an investigative tool, and how is the Service responding to these challenges?

To answer these questions, SIRC examined the role and contribution of a specialized unit created in 2001 SIRC also looked at the activities of to understand how CSIS uses the Internet to enhance its traditional investigative methods. Finally, the report discusses issues related to CSIS's use of the Internet, such as how radicalization and the Internet is increasing CSIS's contact with youth, as well as the nature and potential volume of information being collected and retained

2 METHODOLOGY AND SCOPE

During the course of its review, SIRC examined an assortment of CSIS corporate and operational information and held briefings

SIRC examined

documents

The review period covers January 1, 2009 to March 1, 2010; however, to provide the proper context for some of the operations, it was necessary to examine earlier documents.

3

In recent years, CSIS has undertaken several initiatives to enhance the value of its operational use of the Internet. Chief among these was the creation of established in 2001 as result of the Service's recognition that the Internet was an important investigative tool.[6]

[6] Internal Audit of File Number: 880-118.

CSIS believes there is no need to have policies designed specifically for operational use of the Internet as an investigative tool, and the Service relies on the application of existing operational policies,

CSIS believes that the same rules that apply to the physical world can also be applied to the Internet.

has nonetheless sought to provide more formal training,

The training manual is an excellent reference tool that contains exercises and comprehensive examples based on real cases. There are step-by-step instructions on different ways of using information, as well as specific instructions, such as how to

Just as the success of a traditional investigation depends on proper planning and critical thinking, so does an Internet-based approach. This type of training document is easy to update - in comparison to policies - and these are, therefore, extremely practical in the context of the ever-changing nature of the Internet.

The documents reviewed support the Service's decision to utilize existing policy to govern CSIS's operational use of the Internet, and there was no indication of a need for more specific policies. Moreover, developed a comprehensive training course and training manuals that are easily updated to reflect the changing nature of the Internet,

3.1 Information Collection and the Value Added to Operations

performs different types of work that help to generate leads and to push investigations forward.

3.3 The Non-traditional Becoming Standard Practice

CSIS classifies techniques as non-traditional but the utility of such methods appears to be growing in importance.

it is important to have the resources in place to deal with the increased workload.

SIRC recognizes the importance of addressing resource issues since such "non-traditional methods" are quickly becoming a regular part of operations and investigations.

5 ISSUES FOR CONSIDERATION

This section discusses two general challenges for CSIS in using the Internet for operational purposes. First, the fact that youth are targets for extremist Internet propaganda, and that almost all youth spend time on the Internet has increased CSIS's exposure to minors. There is also a great deal of open source information available on the Internet that is very easily accessible, which underscores the importance of applying the "strictly necessary" criterion to the collection and retention of information from the Internet.

5.1 The Youth Challenge

CSIS interactions with young Canadians will no doubt increase as the Internet continues to be a prominent radicalizer of youth. Indeed, many of the products that have been put on the Internet for recruitment or radicalization purposes are designed to attract the youth market. "With online propaganda that is often flashy, hi-tech, and interactive, the Internet has helped enable violent Islamists to deliver this message in a way that appeals to increasingly younger demographics."[42]

In its review, however, SIRC came across several instances where CSIS collected and reported on information pertaining to minors,

the volume of information pertaining to young people being entered – and therefore permanently retained - in operational reporting, is on the rise.

[42] "Violent Islamic Extremism, the Internet and the Homegrown Terrorist Threat", Majority and Minority Staff Report, May 8, 2008, p. 3.

CSIS should impress upon its employees the need to exercise added caution when collecting and retaining information relating to a youth.

5.2 Information Overload: Finding and Reporting What's Important

Although a great deal of open source information is available, it should still be subject to the same "strictly necessary" test as information received from other sources.

The Internet offers vast amounts of open source information.

This requires CSIS to pay strong consideration to the "strictly necessary" criterion. This issue is a concern from a legal point of view,

6 CONCLUSION

SIRC's conclusion is that CSIS's approach, in terms of policy and procedure, appears to be sound, and allows for the flexibility required to adapt to the challenge of a changing technological landscape. Issues to consider, however, include CSIS's interaction with youth due to this group's use of the Internet and the challenge of collecting and retaining only information that meets the "strictly necessary" test.