F16

Security Intelligence Review Committee

Comité de surveillance des activités de renseignement de sécurité

PROTECTED - PERSONAL INFORMATION

File No.: 1463-2/12-4

February 21, 2012

Dear

RE: REQUEST FOR DOCUMENTS UNDER THE *ACCESS TO INFORMATION ACT (ATI Act)*

This is in response to your request received on February 13, 2012 by the Security Intelligence Review Committee (Review Committee).

You requested a copy of the Review Committee's report entitled "Review of CSIS Use of Disruption to Counter National Security Threats (SIRC 2009-05)".

Enclosed is a declassified copy of the requested document. Please note that some information in the attached records has been exempted under one or more of sections 13(1) and 15(1) of the *Access to Information Act*.

Please be advised that you are entitled to complain to the Information Commissioner concerning the processing of your request within sixty days of the receipt of this notice. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:

P.O. Box / C.P. 2430, Station / Succursale "D"
Ottawa, Canada K1P 5W5
Tel: *613* 990-8441 Fax: *613* 990-5230

0606/12

PROTECTED -
PERSONAL INFORMATION

Information Commissioner
Tower B, Place de Ville
112 Kent Street, 22nd Floor
Ottawa, Ontario
K1A 1H3

We trust the foregoing to be safisfactory.

Yours sincerely,

Sylvie E. Roussel
Senior Counsel and
ATIP Coordinator

Encl.: (1) - Declassified copy of SIRC Study 2009-05

TOP SECRET

File No.: 2800-150
(TD R496)

CSIS'S USE OF DISRUPTION TO COUNTER NATIONAL SECURITY THREATS

(SIRC STUDY 2009-05)

Security Intelligence Review Committee
June 2, 2010

TABLE OF CONTENTS

1 INTRODUCTION 2

2 METHODOLOGY AND SCOPE 3

3 WHAT IS DISRUPTION? 4
3.1 Why was disruption used against 6

4 A NEED TO ACT? 8
4.1 Why is CSIS's use of disruption of concern? 8
4.2 The evolution of security intelligence 11

SUMMARY OF FINDINGS 14

SUMMARY OF RECOMMENDATIONS 15

1 INTRODUCTION

This review explores specific investigative activities by CSIS and the implications of these activities for the Service.

Whenever CSIS conducts investigations, an intended or unintended consequence can be to counter – or disrupt – a threat to national security. For instance, making it generally known to targets that their activities are being investigated can reduce the likelihood that the targets will continue with their plans. The Service regards these methods to be in accordance with the *CSIS Act*.

SIRC understands that countering or disrupting is part of investigating threats to national security, and may at times be necessary to protect Canadians. However, our review raises four issues with respect to the Service's use of disruption that the Committee believes require further consideration. First, disruption potentially overlaps with efforts already exercised by police agencies in Canada. Second, although CSIS's mandate under s.12 does not explicitly prohibit the use of disruption, neither does the authority to collect and analyse intelligence and report to and advise the Government of Canada (GoC) thereon, appear to capture such activities. Third, SIRC believes that ministerial knowledge of CSIS's use of disruption would be appropriate in certain circumstances. Fourth, there are no CSIS guidelines to help with the design and implementation of disruption operations, or to prepare for the potential consequences of such investigative activity.

The following study examines the Service's use of disruption against a threat. Section 3 examines the meaning of disruption, including why the Service selected this measure Section 4 revisits some of the cautionary arguments made by the McDonald Commission of Inquiry that helped create CSIS as a civilian agency devoted to intelligence collection and dissemination.

2 METHODOLOGY AND SCOPE

This review examined CSIS's investigation of a threat to national security, focussing on 'disruption'

During the course of its review, SIRC examined a wide assortment of CSIS corporate and operational information, in addition to holding six meetings with various operational Branches and support services.

The review period covers January 1, 2006 to December 31, 2008.

3 WHAT IS DISRUPTION?

During the Cold War, Canadian intelligence activities were directed at understanding the threat from the Soviet Union. This threat offered considerable stability and predictability: the enemy was known, their intentions were detectable and counterintelligence (CI) methods remained largely the exclusive domain of intelligence professionals. This stands in contrast to contemporary terrorist threats, where enemies are hidden, their intentions are often unclear and counterterrorism (CT) measures frequently require close collaboration among intelligence and law enforcement personnel – a requirement that has become increasingly prominent with the introduction of the *Anti-Terrorism Act*. This complex threat and legal environment means that CSIS may consider activities that extend beyond traditional collection and analysis, including dissuading targets from carrying out threat-related activities

It is

also possible that disruption may occur unintentionally, could dissuade an individual from pursuing future threat-related behaviour even though that result was not intended.

The Service recognizes that disruption is an activity that departs from typical forms of information collection, and that certain risks must be managed when undertaking this investigative activity. As CSIS noted to SIRC when describing the broader ramifications of disruption:

> Less tangible is whether our actions push some people to radicalize, but our assessment is that it discourages radicalization in most people.

As explained by a Service employee during testimony before a Commission of Inquiry, because information is collected by the Service under a lower threshold than in criminal investigations, it is not always possible for police to use CSIS intelligence. As such, this can create an impetus to divert an investigation's focus from prosecution to disruption.[6]

6 CSIS DDO testimony, Commission of Inquiry into Actions of Canadian Officials in Relation to Maher Arar, "Volume 1: Report of the Events Relating to Maher Arar: Factual Background," Minister of Public Works and Government Services, 2006, p.414, note #15.

3.1 Why was disruption used

the Service interviewed people identified as being possibly connected to or as having access to information of relevance. For instance, approached almost individuals who were
Although the primary goal was to collect intelligence from those with possible knowledge of the threat, the Service also hoped to prevent future threat-related activity.

SIRC's review also found that, CSIS has prioritized the need to develop intelligence on the role played as well as to learn the intent That said the Service had just begun to increase its foreign investigative activities

As a result, CSIS could not independently corroborate warnings that Canada might be targeted

Because the date for the action was quickly approaching, the Service expressly set out to disrupt the threat environment.

4 A NEED TO ACT?

The Service maintains that disruption is on a continuum of talking to people when investigating threats to national security, and therefore is in accordance with the Service's mandate. When asked about the possible negative consequences of disruption, CSIS responded that to mitigate community concerns "we always accurately state that we are investigating threats to the security of Canada". Although SIRC understands that disruption is part of a continuum of the Service's investigative activities, the Committee is concerned with ensuring that proper guidance and accountability structures are in place to direct the Service's use of this investigative activity. This is particularly relevant in today's complex threat environment in which there is an increasing convergence between the collection of intelligence and the enforcement of anti-terrorism laws.

4.1 Why is CSIS's use of disruption of concern?

SIRC's first concern is that disruption potentially duplicates actions that are already executed by law enforcement agencies. Since 9/11, there has been a general trend towards the adoption of "an integrated national security framework", as outlined in the Government's national security policy.[23] This policy underscores the importance of connectivity between threat assessments and communicating such information to first line responders such as law enforcement.[24] Therefore, when the Service engages in disruption without the full coordination of the police, it is unclear if this is consistent with the emphasis of the Government's national security policy, which is supposed to create a "clear and effective approach to security" among the various federal departments and agencies which have different responsibilities.[25]

---

23 Department of Public Safety Document, "Securing an Open Society: Canada's National Security Policy," April 2004, p.9. Located at: http://www.publicsafety.gc.ca/pol/ns/secpol04-eng.aspx

24 Department of Public Safety Document, "Securing an Open Society: Canada's National Security Policy," April 2004, Section on Protection and Prevention Capability. Located at: http://www.publicsafety.gc.ca/pol/ns/secpol04-eng.aspx

25 Department of Public Safety Document, "Securing an Open Society: Canada's National Security Policy," April 2004, p.1. Located at: http://www.publicsafety.gc.ca/pol/ns/secpol04-eng.aspx

Concern over the phenomenon of 'mandate creep' is not new. Over a quarter of a century ago the former RCMP Security Service believed that because prosecution could be applied only after offences were committed, law enforcement was an inadequate means of effectively preventing acts of violence. For this reason, the Security Service took upon itself the responsibility to be proactive and to develop threat countermeasures.[26] The McDonald Commission commented that the use of disruptive or counter measures were potentially problematic for those involved in collection and analysis because:

> The collection of information, and its assessment and transformation into intelligence, may be said to be part of the countering (i.e. disruption) process, in the sense that without collection and assessment nothing can be done, although to describe collection and assessment as countering is to expand the definition of the term beyond its real limits.[27]

The Service notes that all of its activities during the disruption campaign were conducted in accordance with its role of obtaining information on a threat, pointing out

However, the Committee believes it is important to differentiate between coordination 'attempts,' and actually succeeding to work together on threat mitigation.

The Committee recognizes that CSIS is not solely responsible for this situation; nonetheless, the very fact that it occurred is cause for concern.

---

26 Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, "Vol. 2 - Part III - Chapter 7: Countering – Security Service," 1981, p.269.

27 Emphasis added. See: Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, "Vol. 2 - Part III - Chapter 7: Countering – Security Service," 1981, p. 273.

The Committee's second observation is that disruption is potentially inconsistent with the Service's Section 12 mandate.[31] For historical context, this issue was raised by the McDonald Commission, which stated:

> the preventing or countering action is taken by a police force or government department exercising an authorized government function, and the security intelligence agency's contribution is confined to its proper role of collecting and reporting security intelligence.[32]

This view of an intelligence agency's role is consistent with the CSIS Director's testimony before a House of Commons Committee. For example, when asked if CSIS has sufficient legislation powers in place to do their job, and if that meant that preventative arrest and investigative hearings were therefore not required, the Director responded:

> I would say that question is more appropriately answered by my colleague the Commissioner of the RCMP. From our perspective, what we try to do is collect information, make it available to the police and others and it's for them to decide whether they're going to do something to disrupt or counter.[33]

Third, **SIRC found that the Minister of Public Safety did not know of the Service's efforts to engage in disruption to mitigate the threat posed** Although the Minister was informed of the threat in February and again in June that same year, in neither case was it made clear that CSIS intended to disrupt the alleged threat. The Committee believes that if CSIS has determined that it is necessary to disrupt threats to national security, then Government should be made aware of this. This issue goes to the heart of ministerial

---

31 Section 12 of the *CSIS Act, 1984* reads: "The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada, and, in relation thereto, shall report to and advise the Government of Canada."

32 Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, "Vol. 2 - Part III - Chapter 7: Countering – Security Service," 1981, p. 274.

33 House of Parliament Document, "Standing Committee on Public Safety and National Security – Testimony by Richard Fadden, CSIS Director," March 11, 2010.

accountability for the Service and therefore should be conducted in accordance with the Minister's full knowledge.

Fourth, the Committee **found that the Service's use of disruption was undertaken in the absence of appropriate guidance.** While there is ample and well-tested CSIS policy on both the conduct of investigations and interviews, the Committee maintains that the absence of clear rules and procedures regarding deliberate and probable disruption is necessary for the Service to account for the use of its powers. SIRC is not convinced by the Service's narrow claim that disruption is simply a "collateral effect"

The Committee believes that CSIS must take further steps to manage such activities, and their outcomes, in the future.

4.2 The evolution of security intelligence

The *CSIS Act* and the *Security Offences Act* were designed to ensure that security offences would be investigated by the police and prosecuted in the courts, while security intelligence collection and analysis would be performed by CSIS. Additionally, Canadians were to take comfort in knowing that Government was clear on where the lines of demarcation lay between law enforcement and intelligence.

The threat of contemporary terrorism has complicated matters for federal departments and agencies. For the Service, this has meant adaptions to novel threat environments, including a progression towards increased foreign activities and investigations within cyberspace. SIRC believes that the use of investigative techniques that result in

disruption is also a manifestation of CSIS's efforts at adapting to the changing threat and legal environment.[38]

Considering that CT operations frequently require close working relationships between intelligence practitioners and their police counterparts, the Committee does not believe it is necessary to determine whether CSIS can or cannot engage in disruption In fact, the Committee understands that disruption is on a continuum with the Service's investigative activities, and may, in some cases, be a desirable and unavoidable outcome to protect the safety and security of Canadians. However, in light of the issues raised above, **SIRC recommends that CSIS seek Ministerial guidance and direction regarding the use of disruption,** including the extent to which 'countering' measures are "proper and acceptable function(s) of a security intelligence agency."[39] Doing so will ensure that the Government is fully aware of the risks involved in some Service investigative activities that result in disruption, allowing Government to guide CSIS on maintaining the distinction between intelligence and law enforcement, as identified by McDonald and underscored by the *CSIS Act*.

Finally, if the Government accepts that the current operational environment requires that the Service engage in deliberate disruption activities, **SIRC recommends that CSIS develop formal guidelines regarding its use of disruption.** Doing so will assist the Service in identifying those investigative activities which either intend to include disruption, or which could result in disruption, and therefore help CSIS to manage any associated risks.

To further assist the Service, SIRC believes that the Service's guidance regarding disruption should provide answers to a number of important questions. Some of these include:

- what kind of proactive activities are acceptable for CSIS to engage in, that go beyond collecting, assessing and disseminating information?
- what are the expressed goals of disruption?
- what must transpire in the operational environment to justify the use of disruption?
- what level of CSIS management approves disruption?

---

38 The Service's Director has recently asserted that intelligence agencies must use "all the tools at their disposal". See: CSIS Document, "Remarks by Richard B. Fadden, CSIS Director to the Canadian Association for Security and Intelligence Studies (CASIS) Annual International Conference," October 29, 2009. See: CSIS website: Speeches and Presentations.

39 Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, "Vol. 2 - Part III - Chapter 7: Countering – Security Service," 1981, p.273.

- what additional training is necessary for CSIS staff to perform activities that are, by design, intended to be coercive?
- how are disruption activities coordinated between CSIS and the RCMP?
- how does CSIS track 'lessons learned' from previous disruption activities and how are these incorporated into future operations?

The Committee believes that addressing these issues will bring appropriate guidance and accountability in situations when the Service's investigative activities result in disruption.

SUMMARY OF FINDINGS

- SIRC found that the Minister of Public Safety did not know of the Service's efforts to engage in disruption to mitigate the threat
- SIRC found that the Service's use of disruption was undertaken in the absence of appropriate guidance.

SUMMARY OF RECOMMENDATIONS

- SIRC recommends that CSIS seek Ministerial guidance and direction regarding the use of disruption.

- SIRC recommends that CSIS develop formal guidelines regarding its use of disruption.

2010-05 0118/12 1463-2/12-1
2010-04 0119/12 1463-2/12-2
2010-02 0120/12 1463-2/12-3
2009-05 FEB 13 2012 0121/12 1463-2/12-4
In Counsel 2/13/12

February 8, 2012

VIA REGULAR MAIL

Alain Desaulniers
A/ATIP Coordinator, Security Intelligence Review Committee
122 Bank Street, 4th Floor
P.O. Box 2430, Station D
Ottawa , Ontario K1P 5W5

Dear Mr Desaulniers,

Re: request for materials

I would like to request copies of the following four SIRC reviews:

1. Review of CSIS's Intelligence-to-Evidence Process (SIRC 2010-05)
2. Review of CSIS's Use of the Internet (SIRC 2010-04)
3. Review of CSIS's Private Sector Relationships(SIRC 2010-02)
4. Review of CSIS's Use of Disruption to Counter National Security Threats (SIRC 2009-05)

If any further information or clarification is needed, please contact me by email at your earliest possible convenience.

Please send the completed request to:

Kind regards,