TOP SECRET

File No.: 2800-164
(TD R516)

DOMESTIC RADICALISATION

(SIRC STUDY 2011-05)

Security Intelligence Review Committee
May 2, 2012

TABLE OF CONTENTS

1 INTRODUCTION

In past years, few threats to national security have provoked as much discussion and consternation as the phenomenon of radicalisation as it relates to Sunni Islamist terrorism. In its latest public Annual Report, CSIS noted that the threat posed by the indoctrination and radicalisation of young Canadians into the violent ideology espoused and inspired by Al Qaeda, which is commonly referred to as "homegrown Islamist extremism", continues to be a key concern; understand the threat posed by the phenomenon of radicalisation in Canada and to also help identify radicalised individuals and groups, and the means by which they have been radicalised.

In addition to its investigative work, CSIS has also engaged with domestic partners as part of a wider government effort to counter the threat. the Director tasked the Intelligence Assessments Branch (IAB) - the branch responsible for strategic analysis and intelligence production - to assess the current state of violent radicalisation

The purpose of this review was to examine CSIS's understanding, investigation and analysis of the radicalisation threat in Canada. SIRC sought to acquire an understanding of the threat, namely what domestic radicalisation means, how it has evolved, and how CSIS has positioned itself to collect intelligence on this threat. To this end, SIRC examined the threat of homegrown extremists, many of whom have had exposure to extremist ideology on the Internet or through contact with other extremists in Canada.

SIRC noted three challenges that CSIS faces in investigating domestic radicalisation: the Internet as a vehicle for radicalisation, the collection and sharing of information on targets and individuals under the age of 18, and the prioritization of multiplying threats related to Sunni Islamist Extremism (SIE). On the second challenge, SIRC noted that although CSIS has amended a number of policies to reflect a higher level of sensitivity in its interactions with minors, it should extend these principles to its practices in relation to the collection and sharing of information pertaining to minors.

SIRC examined how CSIS analyses the phenomenon of domestic radicalisation, so as to broaden its understanding of this process and advise government. SIRC focussed on the work undertaken by IAB, both in terms of its participation in a wider Government approach to countering violent extremism, as well as its analytical products.

2 METHODOLOGY

For this review, SIRC examined operational and analytical documents, namely operational reporting, human source files, CSIS policy, IAB reports, as well as documents related to CSIS's cooperation with other federal government departments, law enforcement and foreign allies. In addition, SIRC was privy to briefings with CSIS Headquarters staff in IAB, as well as management and operational staff in

SIRC focused on the Service's investigation of Al Shabaab in order to gain an in-depth understanding of a homegrown Islamist extremist threat, recognizing that it is not necessarily representative of the wider SIE threat picture. The Al Shabaab investigation was an ideal case study given this group's proven ability to recruit Western youth of predominantly Somali ethnicity, including Canadians, to its violent extremist ideology.

The time period of this review ran from January 1, 2008 to December 31, 2010, although key developments that occurred outside the period were taken into account in order to provide the most up-to-date picture of CSIS's investigation and analysis of the threat of domestic radicalisation.

3 OVERVIEW OF THE THREAT

The term "radicalisation" has been prevalent in past years in media and government circles, as well as academic discussions of terrorism. The term is generally used to refer to the process by which an individual comes to legitimize the use of violence to further political goals.[1] The Government of Canada's priority is to find ways to stop or prevent the radicalisation process in order to reduce the likelihood of terrorism in Canada and/or Canadians being involved in terrorist activity abroad. This requires a whole of government approach, spearheaded by Public Safety Canada, whose first step is to understand the overall phenomenon and process of radicalisation.

As Canada's only security intelligence agency, CSIS has an important role to play in broader government initiatives related to the threat of radicalisation. In investigating this threat, CSIS uses a working definition of "radicalisation" in the domestic context, which encompasses the "transition from moderate beliefs to extremist beliefs which legitimize violence to undermine democratic order or legal systems." Therefore, the focus of CSIS investigations is on the threat once the radicalisation process is complete – that is, the violence itself and the threat it poses to Canadian national security. CSIS recognizes that fundamental religious beliefs do not necessarily constitute a threat to Canadian national security; rather, it is concerned with the violence that may be associated with such extremist beliefs.

Multiple factors may contribute to the radicalisation process, and each individual's path is unique. Still, CSIS has endeavoured to identify patterns or markers that may help signal to them when a person may be at risk. IAB, where the phenomenon itself is being analysed. IAB has found that overall, Canadian Islamist extremists come from a variety of ethnic, family and socio-economic backgrounds, and there is no profile for Islamist extremism or radicalisation. In short, CSIS concurs with a prevailing opinion that it is unlikely that a model of radicalisation will ever be achieved.[3]

[1] CSIS has looked at the phenomenon of radicalisation in the context of many of its investigations since its inception in 1984 (for example, the Sikh extremism threat in the mid to late 1980s).

[3] CSIS IA 2010-11/116 A Study of Radicalisation: The Making of Islamist Extremists in Canada Today (March 3, 2010)

3.1 Investigative Response to Threat

SIRC found that domestic radicalisation is not a stand-alone issue, but one component of CSIS's investigations on threats to national security, with Sunni Islamist Extremism (SIE) being the primary example. Radicalisation, through this lens, is one part of the overall SIE threat picture which has evolved over this past decade. The primary threat of SIE has shifted from non-Canadians abroad seeking to carry out an attack on Canadians abroad or on Canada, to Canadians joining terrorist organizations abroad and attacking other countries, Canada or Canadians, to anyone who undergoes radicalisation within Canada and then seeks to carry out violence in Canada or abroad.[4]

Al Shabaab provides a case in point: this terrorist group has attracted, or recruited, Canadians and Canadian residents; it possesses a domestic and an international component in the form of Canadians radicalising at home and travelling abroad to Somalia to fight and/or train; and represents a concern

Internally, CSIS's investigative response to radicalisation has been evolving to fit operational requirements.

Yet, the threat of radicalisation is still very much front and centre

[4] This latter incarnation is the one most often referred to when CSIS uses the term "domestic radicalisation."

At the same time, there are organisations, such as local police forces, who have outreach models already in place. CSIS recognizes the importance and benefits of building on these efforts, from both an expertise and resource perspective.

SIRC supports the Service tapping into resources that are already in place, and therefore not replicating the work that is already being done by law enforcement and community groups. Domestically, CSIS is working with the Canada Border Services Agency (CBSA) in an effort to keep out those individuals who wish to enter Canada to recruit or proselytize for extremist purposes. Although fundamental religious beliefs on their own do not constitute a threat,

Internationally, the complex nature of the "borderless" radicalisation threat also requires CSIS to meet the challenges of collecting and sharing intelligence with foreign counterparts.

4 INVESTIGATIVE CHALLENGES

4.1 The Internet

Although factors related to the process of radicalisation in Canada include charismatic leaders, peer groups and family members[13], the Internet has been described as "a game changer", in part because it has enabled the quick spread of extremist ideology to an international audience.[14] There has been a trend whereby

become radicalised almost entirely online, without a great deal of face-to-face contact with others.[15] This does not mean these individuals do not interact with others (i.e. they are not truly "self radicalising");

the ever-increasing volume of online threat-related activities have created a significant investigative challenge for CSIS.[17]

Islamist extremists use the Internet to engage in threat-related activities (i.e. accessing jihadi websites, posting extremist comments, viewing extremist literature, etc.).[18]

[13] Briefings (August 24, 2011) and (September 22, 2011).

[14] CSIS Intelligence Assessment 2010-11/67A Islamic Extremist Use of the Internet.

[17] SIRC Briefing with (August 24, 2011).

[18] CSIS Intelligence Assessment 2010-11/67A Islamic Extremist Use of the Internet.

Monitoring online activity is resource-intensive, and the Service recognises that many individuals who appear to have radicalised online pose no actual threat.

In order for CSIS to target someone based on their online activities, there needs to be reasonable grounds to suspect that the person is involved in actual threat-related activities,

Yet, when there is little real world interaction, it may be difficult to investigate these activities through traditional methods, such as physical surveillance. As a result, CSIS may decide to apply for a warrant earlier in the investigative process to avail itself of more intrusive powers and tools needed to push its investigation forward.[22] Even in such cases, in order to get warrant powers, the Service must demonstrate convincingly that these intrusive powers will further an investigation, and that other investigative methods have been tried and/or were deemed not likely to succeed. In short, CSIS must show that they have not "rushed to the court without doing any legwork first."[23]

The *Thresholds for Investigating Internet Based Jihadis,* written in consultation with Legal Services, is a useful tool in assisting investigators to determine whether to target an individual and whether there is justification for a warrant against an individual based on their online activities.

SIRC supports CSIS's efforts to exhaust less intrusive means of investigation before proceeding to a Section 21 warrant application with respect to investigations that have a heavy online component.

[22] SIRC Briefing with (August 24, 2011).

[23] CSIS Document: Thresholds for Investigating Internet Based Jihadis.

4.2 Youth Radicalisation and Violence

Demographics in communities that may be at risk of radicalisation and recruitment mean that CSIS is very likely to come into contact with an increasing number of underage persons as individuals of concern, targets,

Dealing with underage persons presents challenges for the Service, both in respect to its investigative approach, as well as practices concerning information collection, retention and dissemination.

In the course of our review, SIRC saw examples of action taken by CSIS in relation to minors and youth.

SIRC found that CSIS showed due discretion and sensitivity in its dealings with underage persons. For example, it responded to the Ministerial Direction on Operations of 2008 calling on CSIS to recognize "that special considerations should be given when dealing with persons under the age of 18" by amending its policies in relation to its interactions with minors; for example, higher levels of approval are required when persons under the age of 18 [33] Still, SIRC believes that there are other areas, namely with respect to information-sharing and operational reporting, to which this consideration should be extended.

There is no clear approval process set out in operational policy when sharing information on minors, particularly with foreign partners.

As CSIS already has clear processes on how to interview and receive information provided by minors, SIRC believes CSIS should replicate a similar process to govern the sharing of information on underage persons, to establish clear lines of responsibility and approval. Therefore, **SIRC**

[33] OPS-100

recommends that CSIS develop a new policy to govern the sharing of information on minors with foreign partners, or amend existing policy on information-sharing, to reflect due sensitivity to youth.

Another issue with respect to information pertaining to minors relates to its collection and retention in operational reporting. Currently, there is no requirement for CSIS to identify clearly in operational reporting that the information contained in a given message relates to a minor. This means that investigators have to "do the math" in analysing reports to determine if the person referenced is a minor, or was at the time of writing of the report. SIRC noted that there is policy on identifying underage persons in certain reports however, everyday messages entered as part of operational reporting do not have the same requirement. **In order to ensure that appropriate attention and sensitivity are given to intelligence on underage persons, SIRC recommends that *all* operational reporting containing information on a minor be flagged as such.**

4.3 Increasing Threats and Competing Priorities

In recent years, CSIS has had to be judicious in its management of resources, especially given the ever-increasing number of threats As a result, CSIS has developed two tools to assist in prioritizing its investigations and associated resources.

[38]

[38] SIRC Briefing with (August 24, 2011).

SIRC concurs with CSIS's conceptualisation of radicalisation as a part of the threat picture and not a driver of investigations in its own right. SIRC's review found that CSIS's investigations did not stray beyond s.12 parameters (i.e. CSIS did not target individuals with extremist beliefs who do not pose a tangible threat);[42] rather, CSIS's investigations remained focussed on threat, with the phenomenon of radicalisation adding a new dimension to its outreach efforts, analysis and advice to government.

[42] SIRC examined the files of targets

5 CSIS'S ROLE IN ADVISING GOVERNMENT

Terrorism is the GoC's top intelligence priority, of which radicalisation is the primary concern. The GoC, through Public Safety Canada, is working to understand and curb the broader phenomenon of radicalisation through the Preventing and Countering Violent Extremism (PCVE) initiative.[43] CSIS has a crucial role to play in this initiative, namely, providing the GoC with information on radicalised individuals who pose a threat to Canada. Although terrorism falls squarely within CSIS's Section 12 mandate, radicalisation, as a process on a continuum, does not. CSIS may legitimately collect on the threat posed by radicalised individuals, but other information, such as "root causes",[44] may fall beyond the scope of the Service's mandate. However, the GoC has provided intelligence priorities and Ministerial Direction to CSIS calling specifically for information to understand *why and how* people radicalise.

CSIS has responded to this direction and has been advising the government on radicalisation, particularly through the Intelligence Assessments Branch (IAB). For example, the Branch's 2010 "Radicalisation Project" was designed to enhance CSIS's analysis of its targets and to provide a picture of risk factors or patterns that would contribute to the wider understanding of radicalisation as a phenomenon. IAB viewed the radicalisation project as an opportunity to "firmly establish the Service's leadership role on radicalisation," and as a strategy to provide "an information framework which the Service can use to understand Islamist radicalisation and therefore be able to best shape intelligence collection, and to support to the absolute extent possible the whole of Government action in the field of countering violent extremism."[45]

There has been acknowledgement within CSIS that there are limitations to the information and advice that CSIS can provide to government on this issue. This limitation is due, in large part, "to the nature of the Service's mandate, which directs it to investigate threats to national security (and hence individuals already showing signs of

[43] Project Report: Sunni Islamist Extremism, Radicalisation and Counter-Radicalisation in Canada, (April 29, 2011), v.17 Final.

[44] IAB provided reasons why CSIS is looking at radicalisation and the importance of understanding the full story *before* the threat. Briefing with IAB (April 20, 2012).

[45] Email from DDG IAB to (November 24, 2010) and Email from DDG IAB to (December, 2010)

violent radicalisation)."[46] CSIS itself is aware of this limitation, pointing out that it has long recognised "both the individual nature of the radicalisation process as well as the difficulty in determining the precise factors/drivers and relative importance of those factors/drivers in each case."[47]

This is an important issue because IAB is not only responsible for advising the GoC on radicalisation,

The IAB radicalisation study identified "gaps" in knowledge related to potential or possible factors in the radicalisation process,

SIRC is concerned that such information pushes the boundaries of the Section 12 threshold.

Moreover, while this collection may serve to provide more contextual advice to the GoC on the radicalisation process, it has caused tension

[46] CSIS IA 2010-11/116 A Study of Radicalisation: The Making of Islamist Extremists in Canada Today (March 3, 2010)

[47] CSIS IA 2010-11/116 A Study of Radicalisation: The Making of Islamist Extremists in Canada Today (March 3, 2010)

SIRC is concerned that, in the search for wider knowledge, may begin to push CSIS to collect information that does not fall squarely within the boundaries of Section 12 threat-related information. This tension is likely to increase as the pressure on CSIS from the GoC to provide insight into the wider phenomenon and process of radicalisation clashes with the limitations of CSIS's mandate and the work of its collectors.

6 CONCLUSION

Overall, SIRC found that CSIS's investigative activities on and analysis of radicalisation have evolved over time to reflect the Service's learning curve on the issue and to exploit available resources more effectively. However, CSIS still faces some challenges including dealing with underage persons, managing the increasing role of the Internet, and finding ways to prioritise targets, investigations, and intelligence requirements.

CSIS "is tasked with investigating individuals and groups that pose a threat to Canadian security and hence deals with individuals whose activities and beliefs are already radicalised.

[52] Clearly, CSIS's contribution to the analysis and discussion of radicalisation is valuable, as its day-to-day work revolves around investigating individuals who have undergone the process.

Radicalisation is one piece of a larger threat picture. Similarly, CSIS's advice to government on the issue of radicalisation should be only one piece - the threat portion - of a larger discussion on the phenomenon.

[52] CSIS IA 2010-11/11 (May 6, 2010) Homegrown Islamist Extremism in the US.