CSIS Threat Disruption in Context

David Hebb
University of Ottawa, Faculty of Law

Introduction

On June 18th, 2015 the controversial anti-terror bill, Bill C-51, was given royal assent. Despite strong warnings about the scope and constitutionality of the bill only minor changes were accepted. This paper explores the statutory and comparative context of the new CSIS threat reduction measures now allowed for under section 12.1 and section 21.1 of the *CSIS Act*. These measures have also been referred to as disruption powers. If treated correctly, these measures may become an invaluable part of Canada's national security architecture. However, ambiguous drafting of the relevant sections have left significant questions as to what threat disruption measures may entail and to what extent they implicate *Charter* rights. That vagueness invites constitutional challenge, and litigation dealing in part with the language of section 12.1(3) of the CSIS has been already been initiated.[1] This paper argues that as section 12.1(3) currently reads, there are serious concerns regarding the rule of law and the independence of the judiciary. In order to ensure that section 12.1(3) is *Charter* compliant, it should be redrafted to remove any mention of a threat reduction measure violating the *Charter* rights of the individual. In the alternative, the government should draft in a clear and comprehensive list of occasion where CSIS may infringe on an individual's *Charter* rights, and in what form that infringement may take.

To begin, this paper will situate the new threat reduction measure mandate against the context of the McDonald Commission and the events surrounding its report. It will then look to

[1] "CCLA & CJFE Mounting Charter Challenge Against Bill C-51" (July 21, 2015) Canadian Civil Liberties Association Website, online: <https://ccla.org/ccla-and-cjfe-mounting-charter-challenge-against-bill-c-51/>.

explore exactly what a threat reduction measure might include, and discuss whether CSIS should have those measures available to them. This paper then conducts a comparative analysis with two of Canada's Five Eyes allies – New Zealand and Australia. Discussion shifts to the potential issues inherent in CSIS being provided with a mandate to take kinetic action. This will include commenting on issues of confliction, redundancy of powers, a lack of effective oversight, and the implications of kinetic action in a foreign context. To conclude, this paper will analyze and rebut the government's positions on the constitutionality of the CSIS threat reduction measure warrants.

Revisiting History

In order to understand the implications of CSIS' new disruption mandate it is necessary to revisit the origins of CSIS and the findings of the McDonald Commission. The commission speaks as to why policing powers and intelligence were separated, and breaks into the roots of the RCMP drama of the late 1970s.

Before the creation of CSIS, the RCMP's Security Service was responsible for Canada's security intelligence. Their conduct became suspect shortly after the FLQ October Crisis and the 1976 Summer Olympics in Montreal, which had become perceived as a failure of the RCMP to provide timely and accurate security intelligence support to prevent terrorist activity.[2] To the contrary, it does not appear that there was any glaring deficiencies in their work. However, this did change the institution culture into what has since been described as 'noble cause corruption'.[3] Noble cause corruption led to the use of what has famously been termed as 'dirty tricks'. These

[2] Craig Forcese & Kent Roach, *False Security, the Radicalization of Canadian Anti-Terrorism* (Toronto: Irwin Law, 2015) at page 39 [*Forcese & Roach*].
3 Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (1981) ("McDonald Commission" or "McDonald Inquiry"), at p. pp. 267,271, 272, 275 and 353-358.

tricks, or countermeasures, included actions such as the exploitation of power struggles, the fraudulent use of funds, arson, and burglary.[4] The RCMP's actions famously include the stealing of membership lists for the Bloq Québécois and the deliberate torching of a barn by an RCMP officer in order to prevent party meetings from taking place. The McDonald Commission was created in response to the discovery of these actions and framed the subsequent debate for reform of Canada's security intelligence.[5]

The McDonald Commission published various recommendations over three reports that delved into the illegal conduct of the RCMP contrary to the rule of law.[6] They found that the RCMP Security Service had partly been enabled to break the law because the matters rarely made it to court. Terrorism cases were often dealt with through active disruption than prosecution. [7] The most significant recommendation from the McDonald Commission for this discussion is that policing and intelligence be separated and neither be allowed to engage in illegal acts.[8] Instead, if agents or officers required the ability to violate the law, the government should enact a specific allowance for that conduct within the relevant legislation.[9] Other recommendations included the creation of a parliamentary committee to oversee the security intelligence sector, the creation of an advisory council, and an appeals tribunal.[10]

The government's response to the McDonald Commission's recommendations was less than enthusiastic - the government received the recommendations, delayed in publishing them, and then seemingly disregarded the majority of it. They tabled Bill C-157, the first attempt to

4 The Law Union of Ontario's Brief to the Standing Committee on Public Safety and National Security on Bill C-51 at 7.
5 Reginald Whitaker, Gregory Kealey, Andrew Parnaby, *Secret Service: Political Policing in Canada: From the Fenians to Fortress America* (Toronto: University of Toronto Press 2012) at 355 [*Whitaker et al*].
6 Rosemary Way, "The Law of Police Authority: the McDonald Commission and the McLeod Report" (1985) 9:3 Dal LJ 683 at 689.
7 *Whitaker et al, supra* note 5 at page 39.
8 *Ibid* at page 356.
9 *Forcese and Roach, supra* note 2 at page 41.
10 *Whitaker et al, supra* note 5 at page 35.

create a civilian intelligence service, which was called an assault on democracy. It included sections that would have allowed for the breaking of law, provided an overbroad definition of threats to the security of Canada, and only allowed limited oversight.[11] The Senate was instrumental in collecting public submissions and bringing the concerns of experts and the public to the table. The committee recommended over thirty amendments. Bill C-157 was ultimately killed and rebirthed into the *Canadian Security Intelligence* Service *Act, 1985*.[12] The *CSIS Act* divested all security intelligence responsibilities from the RCMP and placed them with the new civilian intelligence agency.

What are Threat Reduction Measures?

Before talking about the desirability of threat reduction, it is important to understand what they are and what they might include. As discussed in the 2009-2010 annual Security Intelligence Review Council (SIRC) report, CSIS has been conducting incidental disruption as part of their investigations for some time.[13] Simply knowing one is being watched by CSIS may be enough to change the path of a radicalized individual. It may also push them further towards radicalization, but an internal report has decided that the net effect has been positive.[14] Further, some investigative techniques may inadvertently alter the path of a developing threat through other unspecified means.[15] More direct disruption or counter threat activity since the creation of CSIS has been conducted by the RCMP. This paradigm was acknowledged and lauded by the previous CSIS Director, Mr. Richard Fadden, in an appearance before parliament.[16]

---

[11] *Whitetaker et al, supra* note 5 at page 360.
[12] *Forcese & Roach, supra* note 2 at page 42.
[13] *Standing Senate Committee on National Defence and Security*, 42st Parl, 2nd Sess, No 35 (20 April 2015) (Michel Coulombe) [*Coloumbe*].
[14] *Forcese & Roach, supra* note 2 at page 246.
[15] Canada, Security Intelligence Review Committee, *Annual Report 09/10, Time for Reflection, Taking the Measures of Security Intelligence* (Ottawa: Public Works and Government Services Canada, 2010) at page 16 [*SIRC*].
[16] *Ibid* at page 17.

In section 12.1 of the *CSIS Act*, disruption powers are labelled 'measures'. Section 12.1 directs that these measures be used against 'threats to the security of Canada'.[17] This term is defined within the Act and includes espionage, foreign influenced activities, violent activities or the support of violent activities for a political, religious, or ideological objective, and covert or unlawful acts intended to lead to the destruction or overthrow of the Canadian government. This definition excludes lawful advocacy, protest or dissent, unless they involve the application of any of the four listed definitions of a threat.[18]

CSIS is able to conduct non-illegal disruption without a warrant so long as there are reasonable grounds to believe the targeted individual or act is a threat. Such an action could include the much discussed ability of CSIS to engage the parents of radicalizing children or other community leaders in a conversation about deterring the youth from proceeding down the path of radicalization. Unwarranted CSIS disruption powers would also likely include the aforementioned incidental disruption effects of investigations. If CSIS seeks to push their disruption into what could be considered illegal or that implicates a Charter right, CSIS must first seek approval from the Minister of Public Safety and Emergency Preparedness, and then argue their case before a Federal Court designate judge in order to receive the warrant.[19] The judge issuing the warrant has the power to reject the request or modify the outer limits of the requested activity as they deem appropriate given the circumstances. For investigatory warrants, designate judges have been more likely to modify the terms of the warrant and provide it than to deny it outright.[20] They may also request that CSIS report back, something that is expected to happen

[17] *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 at section 12.1 [*CSIS Act*].
[18] *Ibid* at section 2.
[19] *Standing Senate Committee on National Defence and Security*, 42st Parl, 2nd Sess, No 35 (2 April 2015) (John Ossoswki) [*Ossowski*].
[20] Justice Mosley, "A View from the Bunker: The Role of the Federal Court in Nation Security" (Talk delivered at University of Ottawa, Faculty of Law, 2015) [*Mosley*].

frequently.[21] Indeed, for some forms of warrants, a report back condition is inserted routinely. For others it is done when deemed necessary. CSIS has thus far complied with such requests.[22]

Warrant requests are presented to the designate judge *ex parte* – or without the presence of the party subject to the warrant. When there are substantive issues of law the court will appoint an *amicus curiae* in order to provide an independent analysis and balance CSIS' position.[23] For example, a 2013 redacted federal court decisions involved the appointment of an *amicus* to assist in the consideration of whether CSIS has a mandate to conduct extraterritorial investigations, and whether the federal court had jurisdiction to issue such a warrant.[24] Specifically in the case of disruption warrant hearings, Federal Court Chief Justice Crampton has stated that an *amicus* will be present.[25] *Amicus* lack most of the rights and special access privileges afforded to the security certificate process' special advocates, but will still provide the designate judge with an element of adversarial process.

The designate judge will process warrant applications as efficiently as possible, but they must also be allowed a minimum of 48 with which to properly consider the application for new warrants.[26] Disruptive action is authorized for up 120 days with the possibility for renewal. The renewal may last no longer than the period originally allowed for in the warrant, and a renewal may only be applied twice.[27] Decisions are not generally published, but if they are of particular interest to the public or in terms of questions of law they may be published in a redacted form.[28]

---

[21] *Ossowski*, *supra* note 19.
[22] Personal communications with law clerk of a designate judge, 2015 [LC*Comm*].
[23] *Ibid*.
[24] X (Re), 2013 FC 1275 at para 9.
[25] Cristin Schmitz, "Chief Justice shows where line is drawn", *The Lawyers Weekly* (3 July 2015) online: < http://www.lawyersweekly.ca/articles/2417> [*Schmitz*].
[26] *LCComm*, supra note 22.
[27] *CSIS Act*, *supra* note 17 at section 22.
[28] *Mosely*, *supra* note 20.

What may actually constitute a disruptive action is more ambiguous. Some guidance is presented in section 12.1(2) to 12.1(4), and section 12.2(1). Disruptive measures must be "…reasonable and proportional to the circumstances, having regard to the nature of the threat, the nature of the measures, and the reasonable availability of other means to reduce the threat," but does not include any law enforcement power.[29] Those measures may not cause death or bodily harm, obstruct or pervert the court of justice, or violate an individual's sexual integrity.[30] The outer limits from section 12.2(1) are actually a mirror of the equivalent measures in the criminal code that allow the RCMP to act illegally in the course of their investigations.[31] The concern that has been raised is that of implied exclusion. If these are the only outer limits for CSIS disruption action, any other conceivable action that does not include or falls just short of those listed grounds is allowable. This allows a great deal of leeway.

A sorely overlooked aspect of these disruption powers is how they allow CSIS to reach outside of their own resources and enlist the aid of other national security organizations or even other private parties. A judge may issue an assistance order which expands the scope of the disruption warrant onto any party that CSIS believes will be able to assist them.[32] This includes the Communications Security Establishment (CSE). CSE has three mandates. Mandate C as detailed in section 273.64(1) of the *National Defence Act*. CSE is to "provide technical and operation assistance" to law enforcement and security agencies in the performance of their lawful duties. Previously this has had CSE assist in investigations and surveillance. With the passing of Bill C-51, threat disruption is a part of CSIS' lawful duties. This brings the significant

[29] *CSIS Act, supra* note 17 at section 12.1(2) & s 12.1(4).
[30] *Ibid* at section 12.2(1)
[31] *Forcese and Roach, supra* note 2 at page 229.
[32] *CSIS Act, supra* note 17 at section 22.3.

technical expertise and ability of CSE to play.[33] It is unclear how comfortable CSE will be in providing disruption assistance due to their predilection for staying out of sight and out of mind as well as the novel nature of legal disruption.

Actions taken by CSIS and those empowered by CSIS warrants may implicate an individual's Charter rights. The exact extent of this implication and potential infringement has been the topic of much discussion, and is one that this paper will continue in following sections. While CSIS is held responsible to SIRC and to the federal court, it is unclear what mechanisms will provide accountability for those who CSIS enlists to assist in its disruption activities. SIRC has trouble 'following the thread' in its investigations from agency to agency. One can only imagine that the thread will stop completely when it enters into the realm of private actors. A search for the outer limit for activities conducted in violation of the *Charter* bears little fruit. The government has explained that one instance where a *Charter* right could be involved is where CSIS needs to interfere with the mobility of a target.[34] They repeated that this would not include being able to detain them, but also denied to include an amendment to that effect saying that it would unduly narrow the tools available to CSIS.[35] There has been little communication from the government on what would constitute an acceptable or unacceptable limitation of *Charter* rights. One method of demarking the outer limit would be through the consideration of precedence, but due to the secret nature of those proceedings there is a real concern about the development of a secret jurisprudence of *Charter* violations. Further, this jurisprudence will be developed without the full advantage of a robust and fair public discussion.[36]

---

[33] See "CSEC Cyber Threat Capabilities – SIGINT and ITS: an End-to-End approach", leaked internal document.
[34] *Standing Committee on Public Safety and National Security*, 42st Parl, 2nd Sess, No 62 (31 March 2015) at 1925 (Mike Duffy) [*Duffy*].
[35] *Standing Committee on Public Safety and National Security*, 42st Parl, 2nd Sess, No 62 (31 March 2015) at 1950 (Ted Falk) [*Falk*].
[36]

Should CSIS have Disruption Powers?

The prospect of CSIS having disruption powers is not a novel issue. It is one that has been considered by SIRC since at least the 2009-2010 annual report. SIRC notes that CSIS was not precluded from disrupting threats by the previous version of the *CSIS Act*. In fact, they state that disruption is simply an aspect of investigating national security threats. Depending on the context, it may even be necessary.[37] SIRC primarily discusses disruption that is incidental to investigation – the indirect disruption that occurs when an individual knows they are being watched, or an activity that dissuades the individual from becoming a threat unintentionally. [38] SIRC articulated concerns that parallel those articulated before committee, but also brought forth more practical legal issues. Specifically, they believed that ministerial authorization or knowledge should be required, and that the development of internal guidelines for the planning and use of disruption would be necessary.[39] It appears that the section 22.1 warrants incorporate that advice, requiring ministerial sign off prior to an application being brought to the court. It is also likely that CSIS has been hard at work developing internal guidelines.

The argument in favour of more direct disruption is not complex. CSIS will at times be better situated to conduct a threat disruption operation due to their familiarity with the threat and their access to secret information about the threat.[40] Former Minister Blaney added to that before the senate committee, stating that CSIS and the RCMP have a different focus. The RCMP is concerned with criminal investigations that lead to a prosecution. Meanwhile, CSIS is engaged at a pre-criminal stage monitoring the threat as it manifests.[41] The new threat disruption powers

[37] *SIRC, supra* note 15 at page 16.
[38] *Ibid*
[39] *Ibid.*
[40] Mike Duffy during National Security Law (University of Ottawa, CML 3356, 2015).
[41] *Ossowski, supra* note 19.

conferred to them allow access to tools and techniques that can be applied to change the path or impede the development of the threat.[42] Further, the cost of disrupting a threat is much less than the cost of mounting a full investigation. If a disruptive action successfully pushes an individual off the path of radicalization, it saves significant amounts of money and the time of agents and officers that can be put towards other threats.

Disruption is a natural evolution of the CSIS mandate in response to an evolving threat environment that provides complications for national security agencies.[43] With the proper safeguards and accountability similar in principle to those around RCMP disruptive activity, CSIS disruption is not undesirable. It represents a valuable tool for inhibiting terrorist activity and disarming threats, and should be considered as part of a much larger system that includes the new information sharing, no-fly list, speech crime, and peace bond provisions from Bill C-51. CSIS threat reduction measures are one tool in a very large tool belt, one that is geared to handle the modern dynamic threat environment.

The Comparative Context

One of the rationales for this amendment was that Canada needed to 'catch up' to its allies in terms of the abilities of their security intelligence agencies.[44] Looking at what tools are available in other Five Eyes and other allied countries may provide some insight into what this entails, and also provide context how certain powers have been treated internationally. Information on the capabilities of a state's security intelligence agencies is not always readily accessible, but some insight can be derived through considering their national security

[42] *Standing Senate Committee on National Defence and Security*, 42st Parl, 2nd Sess, No 33 (30 March 2015) (Steven Blaney) [*Blaney*].
[43] *SIRC, supra* note 15 at page 17.
[44] *Blainey, supra* note 41.

legislation. Choosing comparable states is not easy - the organization of national security agencies is far from standard. Further, there is hardly room in this paper to consider all of them. A thorough comparative analysis with a range of other countries is for another paper. For now, this paper will consider New Zealand and Australia's security intelligence agencies and contrast them to CSIS.

Australia's equivalent to CSIS is the Australian Security Intelligence Organization (AISO). Their mandate is to collect intelligence and conduct investigations on the actions of Australian citizens, along with the familiar mandate of conducting security assessments and providing advice. A crucial aspect of their guiding legislation, the *Australian Security Intelligence Organization Act (1979)*, is section 17(2). This section explicitly states that AISO is not in the business of carrying out or enforcing 'measures' in the name of security.[45] This seems to bar AISO from conducting CSIS style disruption.

AISO has a similar warrant system to CSIS, though the legislation is much more specific as to what the warrant may be used for. There are separate sections of the *AISO Act* dealing with search warrants, computer access warrants, and various other warrant authorized activities such as the use of listening or tracking devices.[46] The first thing to note with these sections is that they all concern the collection of information, and not the active disruption of threats. However, AISO receives access to two additional warrants in relation to terrorism offences – a questioning warrant, and a questioning and detention warrant.[47] Even though the later of these warrants do allow for the detention of a citizen, the warrant is only provided in order to assist AISO in

[45] *Australian Security Intelligence Organization Act 1979* (Cth), section 17(2) [*AISO Act*].
[46] *Ibid* at sections 25, 25A, 26A.
[47] *AISO Act*, *supra* note 45 at section 56.

collecting intelligence when other methods of collection are ineffective.[48] Further, the individual must be taken into custody by a police officer, and they may be in custody for a maximum of 168 hours.[49] There is a mild disruptive aspect to the warrant, but only insofar as it ensures the protection of evidence, preventing the alerting of an accomplice as to the existence of an investigation, or if there is a risk of non-appearance before a prescribed authority.[50]

Since CSIS' mandate has been expanded to include international operations through Bill C-44, another comparable Australian organization is the Australian Security Intelligence Service (ASIS). They are governed by the *Intelligence Services Act (2001)*. Their mandate it set out in section 6 of the Act, and is comprised of six subsections. ASIS' functions are to obtain intelligence about foreign agencies or people, to provide that intelligence to the government, to conduct counter-intelligence, to work with other security services or agencies from other states, and to undertake other activities as directed by the minister.[51] Caveats to the last function include a duty of consultation with other affected ministers, that the action taken must be relevant and reasonable to the objective to be achieved, and such actions may only happen outside of Australia.[52]

AISO's terrorism warrants received the criticism of being oppressive and lacking adequate oversight, especially as it pertains to targeting non-suspect civilians.[53] These concerns have persisted through the 15 month march through parliament and despite a sunset clause set to expire in 2016 pending renewal.[54] Bill C-51 lacks that thorough consideration through

---

[48] *Ibid* at section 34F(4).
[49] *Ibid* at sections 34G(3), 34(g)(4)(c).
[50] *Ibid* at section 34F(4)(A-D).
[51] *Intelligence Services Act 2001,* (Cth) at s 6(1) [*ISA*].
[52] *Ibid* at s 6(2).
[53] Lisa Burton, Nicola McGarrity, George Williams, "The Extraordinary Questioning and Detention Powers of the Australian Security Intelligence Organization" (2015) 36 Melb U LR 415 at 417 [*Burton*].
[54] *Burton, supra* note 53 at page 418.

parliament and a similar sunset clause. Further, there is no express rejection of detention being within the ambit of CSIS' disruption powers. Government witnesses and committee members were consistent in denying that CSIS would be allowed to detain, and section 12.1(4) was included in part to preclude CSIS from being able to arrest or lawfully detain an individual.[55] This overlooks that not all detention is pursuant to a police power. In fact, as mentioned before, a proposed amendment that detention be specifically bared was rejected on the grounds that it would unduly narrow the tools available to CSIS contrary to the intention of the Bill.[56] This was justified again with reference to hypothetical operations in which CSIS would find it necessary to interfere with the movement of an individual.[57] That does not change the fact that detention is not provided on a list of prohibited actions or otherwise ruled out in any other way, and is thus technically available.

The overlap CSIS has with ASIS is tempered by their scope of operations. ASIS is a foreign intelligence agency that has the ability to take 'measures' as prescribed by the Minister outside of Australia. CSIS has that mandate as well, but their use of 'measures' applies within Canada as well. This makes them unique in relation to Australian security agencies.

New Zealand has a similar legislation structure to Australia for domestic security intelligence agency, the New Zealand Security Intelligence Service (NZSIS). Their mandate is functionally similar – NZSIS is to collect intelligence, advise the government, and conduct security clearances.[58] It also includes an almost identical clause to section 17(2) of the *AISO Act*. It is outside of NZSIS' mandate to enforce security measures.[59] *The New Zealand Security*

[55] *Standing Committee on Public Safety and National Security*, 42st Parl, 2nd Sess, No 62 (12 March 2015) at 1935 (Roxanne James).
[56] *Falk*, *supra* note 35.
[57] *Duffy*, *supra* note 34 at 1940.
[58] New Zealand Security Intelligence Service Act 1969 (*NZ*) 1969/24 at s4(1) [*NZSIS Act*].
[59] *Ibid* at s4(2).

Intelligence Service Act (1969) provides much detail in terms of intelligence warrants, but does not allow for NZSIS to take an active disruption role. The only discussion on prevention takes the form of information retention in the context of preventing or detecting a serious crime.[60] There is no argument by analogy to be found for CSIS disruption powers in NZSIS, although the government did say 'most' of Canada's allies rather than 'all' when referencing the need to catch up.

The issue appears to be that the government was not exclusively looking at other nations' domestic security intelligence agencies. This is understandable to the extent that each nation has a different national security portfolio and there are not always direct parallels. Canada does not have a dedicated foreign intelligence service. Domestic and foreign security intelligence appears to have been combined under one roof. This is significant because the scope of powers made available to foreign intelligence services is often more vast than those afforded to their domestic counterparts. As far as this comparative analysis went, disruptive powers or measures are only authorized outside the border of the state. There was no organization surveyed that had such *carte blanche* disruption powers within the territorial bounds of its home state. While Bill C-51 and Bill C-44 appear to have made CSIS into an impromptu foreign intelligence service, there is a lack of a separation of powers in relation to those two functions that is seen elsewhere. Further, no foreign agency considered in this paper had the ability to act contrary to their home state's constitution.

The argument by analogy made by the government would bring more weight is CSIS were divided into foreign and domestic components, each with their own mandates and legislation. The more controversial threat reduction measures would be less novel in the context

[60] *NZSIS Act*, supra note 58 at s4H(1).

of a foreign service. An alternative idea would be to create a completely separate foreign intelligence service, but this is an option that has been rejected in the past.[61] As it stands now, CSIS' mandate is new and radical by comparative standards.

Critiques of CSIS Disruption

Reuniting Policing & Intelligence

The foremost criticism about CSIS receiving threat reduction powers is rooted in the recommendations of the McDonald Commission. At the forefront of the report was the civilianization of the intelligence. This required the separation of policing powers from security intelligence responsibilities. Civilianization was the impetus for the creation of CSIS. Disruption powers are at least in part a policing power, and questions are raised about whether the government has chosen to tacitly ignore the lessons of the McDonald Commission. This criticism is not completely true. Many of the issues that led to abuse of powers by the RCMP in the late 1970s have been remedied at least in part through the procedural and structural guidelines surrounding CSIS threat reduction measures. It is unlikely CSIS would advance an application that they do not believe will be accepted by the judge. This suggests that CSIS will conduct its own weighing process prior to application on the reasonableness and how necessary an action is. However, not every disruptive action is going to proceed through that avenue.

Confliction between RCMP and CSIS investigations was an issue present before the introduction of CSIS' threat disruption mandate, but now the stakes are higher. CSIS and RCMP persist in a system of parallel investigations. CSIS provides the RCMP with an advisory notice

[61] Gloria Galloway, "No new agency for foreign intelligence, top spy says". *The Globe and Mail* (May 29, 2007) online: < http://www.theglobeandmail.com/news/>.

disclosing their investigation when police involvement becomes necessary.[62] The Air India Inquiry had much to say about this mode of investigation and transfer. Concurrent investigation is a part of the system, but concurrent disruption by both parties has more serious implications. This interference could have the effect of tainting a criminal terrorism investigation and preventing prosecution. Further, there are no clear protocols for passing off a CSIS investigation that has involved disruption to the RCMP for the purposes of it being carried to court. Issues of evidence and the handling of secret information have yet to be dealt with.[63] CSIS and the RCMP will have to rely heavily on their pre-existing de-confliction mechanisms, as well as any developed in response to this new paradigm.

Redundancy

Many of the uses for the CSIS disruption warrants described during committee overlap with powers conferred through different legislation. For example, the new speech crime laws will allow for the removal of a website that violates its terrorist propaganda prohibition. The same effect could also be reached through a CSIS warrant where CSE is tasked with removing that website.[64] Alternatively, rather than placing a person on the no fly list CSIS may instead simply cancel the ticket or block their payment. This has the effect of superseding the more transparent and already legal method.

Will CSIS reach for such tools when they already have access to those powers through warrants? That depends on how they construe section 12.1(2) of the CSIS Act. This section requires that CSIS only take actions that are reasonable and proportional, but also that

[62] *Forcese & Roach, supra* note 2 at page 11.
[63] *Forcese & Roach, supra* note 2 at 259.
[64] *Ibid* at page 250.

consideration is paid to "…the reasonable availability of other means to reduce the threat."[65] This section falls short of placing a positive obligation on CSIS and the federal designate judge to seek out or prefer those methods. Proceeding through otherwise available means will at times be preferable. When a person finds out they are on the no-fly list they are at least notified and given the opportunity to appeal their listing. How effectual that appeal process is would be the topic for another paper. Further, proceeding through the new speech crime provisions introduces the courts earlier in the process. It is understandable that in order to preserve the integrity of an ongoing investigation CSIS may need to proceed clandestinely. This is a consideration the designate judges will need to address in their weighing of section 12.1(2).

Review and Oversight

Review and oversight are two distinct concepts that need to be clearly defined. To have review is not to have oversight, and the opposite is true as well. Review comes from the careful consideration of events after they are passed. Oversight concerns ongoing events where a third party is able to execute a command and control function.[66] Oversight is the more complicated of the two to implement effectively as it involves keeping an eye on intricate moving parts.[67] Most of the discussed measures to provide accountability to CSIS have been in the realm of review. The proposed committee of parliamentarians to serve as an intermediary between Canada`s national security apparatus and parliament is a prime example. In contrast, Justice John Major`s suggestion of a national security advisor that can co-ordinate security efforts and see beyond the silos would be more in the vein of oversight. As it currently stands, review over CSIS is

[65] CSIS ACT, supra note 27 at s12.1(2).
[66] *Forcese & Roach, supra* note 2 at page 399.
[67] *Standing Committee on Public Safety and National Security*, 42st Parl, 2nd Sess, No 61 (26 March 2015) at 1840 (Tom Stamatakis).

conducted by SIRC – an independent third party organization that has access to secret information and prepares annual reports for parliament.

While no longer active, the inspector general for CSIS used to be the eyes and ears of the Minister of Public Safety within the organization. Since the position's abolishment, the responsibilities of the inspector general have been subsumed into SIRC. This has expanded SIRC's mandate into the area of certification as well as other various responsibilities formerly held by the inspector general. SIRC now vetting the director of CSIS' annual report to the Minister of Public Safety for accuracy and integrity each year.[68] SIRC has further expanded its review capability to include ongoing operations, which begins to present a limited form of oversight to their activities.[69]

In SIRC`s annual reports, they conduct a review of certain CSIS operations and assess their conduct. A part of these reports is making recommendations to CSIS in response to the activities they consider. CSIS is not obliged to implement any of these recommendations, but they have been used within the service to improve their methodology and efficiency.[70] SIRC reviews operations that are already publically notorious, are high risk, or involve new forms of activities.[71] The latter category in this list suggests that SIRC will be paying close attention to CSIS threat reduction activities.

SIRC is the only form of review CSIS currently has asides internal mechanisms. This is somewhat bolstered by the warrant requirement in 12.1(3) of the CSIS Act. However, this only amounts to limited judicial oversight.[72] In addition to the aforementioned procedural issues

[68] SIRC representatives during National Security Law (University of Ottawa, CML 3356, 2015) [*SIRC NSL*].
[69] *Ibid.*
[70] *Coloumbe*, *supra* note 13.
[71] *SIRC NSL*, *supra* note 68.
[72] *Standing Senate Committee on National Defence and Security*, 42st Parl, 2nd Sess, No 34 (2 April 2015) Craig Forcese).

mentioned above, there is limited opportunity for review after the warrant process. It appears CSIS will be being asked to report back frequently on the execution of their warrants, but such warrants are unlikely to see daylight in subsequent criminal proceedings. Perhaps the only notable instance of a CSIS warrant making it to court came during the VIA Rail bombing prosecutions. Information collected from a CSIS investigatory warrant was used to justify an RCMP communication intercept warrant, and the validity of the CSIS warrant was brought into question by the defence.[73] With a disruption warrant, there will be no chain of documents leading to CSIS from an RCMP action. In fact, the target may never know that action was taken against them.

CSIS only requires a warrant where there are reasonable grounds to believe that one is required.[74] Any action that falls just short of being illegal or in violation of an individual's *Charter* rights may proceed without the issuance of a warrant. This places significant interpretive power in the hands of CSIS agents on issues that may have a significant impact on the lives and rights of those they are investigating. In essence, these powers ask CSIS agents to have perfect judgement as to what does and what does not require a warrant. This is not only a troubling situation, but one that is unfair to CSIS. Legislation should not be drafted to require perfect judgement to carry out its intentions. A more appropriate standard would be reasonable suspicion. While not a panacea, this would ensure CSIS received warrants for even potentially legally troublesome actions while still allowing them to conduct activities such talking to parents and overt surveillance efficiently.

---

[73] See "Via Rail plot trial: jurors reach partial verdict after deliberations" *CBC News* (18 March 2015) online: <www.cbc.ca/news>. RCMP warrant was received based on information from a CSIS intercept warrant, defence sought access to the CSIS Warrant material.
[74] *CSIS Act*, *supra* note 17 at s21.1(1).

Extraterritorial Application

CSIS' mandate was extended to include operations outside of Canada through Bill C-44. This expansion is all the more dramatic with the introduction of disruption powers that have the ability to disregard not only Canadian law, but foreign and international law as well with the blessing of a warrant.[75] The discovery of CSIS breaking laws within another sovereign nation could be diplomatically complicated for Canada. Further, certain members from the RCMP have voiced concern that CSIS activities abroad may negatively affect the carefully cultivated relationships they have with foreign police services. Time does not have to be turned back very far to see how this manifests. It was recently discovered that CSE was conducting illicit activities around Brazilian economic interests, and this placed a great strain on the already icy Brazilian-Canadian relations.[76] It would not be controversial to say that most countries allow their agencies to conduct somewhat clandestine and illicit activities upon occasion, but Canada is one of the few with the inclination to codify that capacity into law.[77]

The Constitutionality of Section 12.1(3)

The most fundamental issue with the new CSIS disruption powers lays in 12.1(3), which allows CSIS to breach Canadian law or the *Charter* with the blessing of a federal court warrant. This section will consider the government position in favour of the constitutionality of section 12.1(3) and then consider the arguments against.

Various government actors, ranging from ministers to Department of Justice lawyers, spoke out before committee in an attempt to validate the position that an *ex parte* and *in camera*

[75] *CSIS Act*, *supra* note 17 at s21.1(4).
[76] Susan Ormiston, "Canada's spying touches nerve in Brazil" *CBC News* (15 October, 2013) online: <www.cbc.ca/news>.
[77] Craig Forcese, "Summary of Concerns with CSIS Act Amendments", *National Security Law Blog* (2 february, 2015) online: < http://craigforcese.squarespace.com/national-security-law-blog/2015/2/2/summary-of-concerns-with-csis-act-amendments.html>.

warrant hearing could constitutionally limit a Charter right. There were two notable lines of argumentation. First, there is the claim that judges have been authorizing reasonable infringements of the Charter for a significant amount of time, and the CSIS disruption warrant operates in a similar fashion.[78] The second is that the judge conducts a section one analysis in considering a CSIS warrant application, thereby avoiding a breach of the Charter.[79]

The first argument, the analogy to other warrants, is only partly correct. The primary difference is that pre-existing warrants operate within the internal hedges of the *Charter*.[80] Section 8 provides the right to be secure against *unreasonable* search or seizure. Section 9 protects against *arbitrary* detention. By comparison there is no such thing as 'acceptable' free speech or 'reasonable access' to mobility rights. A warrant is essentially a pre-ruling or certificate of constitutionality that a law enforcement officer may rely on when conducting a search or an arrest. 'But for' the warrant, the action would be unconstitutional.[81] Section 12.1(3) of the *CSIS Act* implicates every Charter right, even those without internal hedges. It also does so in a different way. The focus is not on requiring that any potential infringement must be reasonable and therefore not an infringement, but rather that any infringement must be reasonable and proportional considering the circumstances. This has the potential to be a genuine limitation of one's rights, and presents a new concept in Canadian law.

This flies in the face of the frequent assurances by government witnesses that no *Charter* rights will be violated by through the application of a CSIS warrant. However, it is one that is supported simply by considering the words of section 12.1(3) and the express rejection of any

[78] *Forcese & Roach, supra* note 2 at page 263.
[79] *Duffy, supra* note 24 at 1925.
[80] *Forcese & Roach, supra* note 2 at page 264.
[81] *Standing Senate Committee on National Defence and Security*, 42st Parl, 2nd Sess, No 35 (2 April 2015) (Donald Piragoff).

attempt to amend the section to ensure that any measures taken will not be in violation of one's *Charter* rights. Government witnesses repeatedly asserted that CSIS warrants could not possible authorize a breach of the *Charter*. If that were true, that would be a great comfort. However, the plan meaning of the wording in section 12.1(3) do no lend themselves well to that interpretation,

> The Service shall not take measures to reduce a threat to the security of Canada if those measures will contravene a right or freedom guaranteed by the Canadian Charter of Rights and Freedoms or will be contrary to other Canadian law, unless the Service is authorized to take them by a warrant issued under section 21.1[82]

This section explicitly says that a warrant under section 21.1 will allow for a breach of the *Charter*. Read in conjunction with the wording from section 21.1 it is clear that a judge can reject or change the proposed action by CSIS, but every indication that this is to ensure the limit is reasonable and not that the action is constitutional.

The section one argument is false for separate reasons. It is not correct to say that a federal designate judge will be conducting a section one analysis. Instead, it would be more correct to say that they are conducting a section one inspired analysis. Section 12.1(3) of the *CSIS Act* lacks the requisite standard of intelligibility that qualifies it for saving under section 1.[83] The average citizen will be unable to make sense of what is allowed by section 12.1(3). It provides little guidance, relying on ministerial discretion and subsequent judicial authorization. Further, the judge will not be ruling on the validity of the section itself, but rather the measures

[82] CSIS ACT, supra note 17 at section 12.1(3).
[83] Forcese & Roach, supra note 2, page 264.

that are being brought forth under its auspices. These considerations all militate against this being a correct application of section one.

Outside of these considerations, section 12.1(3) provides more fundamental obstacles. It runs against the recommendation of the McDonald Commission that neither police force nor security intelligence service be allowed to break laws. It also violates the rule of law, the independence of the judiciary, and misconstrues the separation of powers. These are observations that have been made by Professor Forcese and Roach, and many others. Judges are charged with the protection of *Charter* rights in the face of encroachment by acts of parliament or other governmental action. That is to say, judges are involved after the government has decided to take an explicit action that may infringe on a claimants *Charter* rights. It is not up to the judiciary to forge those limitations themselves. It is asking them to step from a judicial review role into one of the executive or legislative creation of limits.

Conclusion – Ensuring the Constitutionality of CSIS Activities

Disruption powers are a novel addition to Canada's national security paradigm, but not an unwelcome one. The ability of CSIS to take action during the pre-criminal stage or to directly avert a threat allows for flexibility in response to the modern dynamic threat environment. However, for such measures to be effective and a long term fixture in Canadian national security law they must be legislated for in a robust and constitutional way. The government has done much to create a strong basis for these powers, but failed in crucial ways to ensure that these sections would withstand constitutional challenge and adequately protect the rights of Canadians. In order to correct this, the government should amend the wording of section 12.1(3) of the *CSIS Act* in order to make it explicit that no *Charter* rights will be violated through CSIS disruption measures. Alternatively, the government should include an explicit list of situations in which a

right may be reasonably infringed and in what manner they may be limited. These changes should be paired with an amendment that any time a Charter right ‘may’ be implicated, a warrant should be sought.

These amendments will proactively protect Canadian’s *Charter* rights, as well as provide an element of intelligibility that will work towards saving the section through a true section one test. It will also leave the executive and legislative role of authoring rights restrictions within the proper bodies, and leaving the designate judges with clean hands. In the face of recent terrorist attacks around the world there is significant temptation to let national security concerns triumph over rights. Canada must resist knee-jerk reactions and patchwork solutions to make an infirm quilt of security.