

The Canadian Security Intelligence Service and the Toronto 18 Case

STEPHANIE CARVIN*

ABSTRACT

While it is well known that the Canadian Security Intelligence Service (CSIS) played a key role in the investigation of the Toronto 18 cases, these activities have been left out of the public record. To provide some context for the other contributions in this study, this chapter proceeds by describing the process by which CSIS conducts counter-terrorism investigations – from initial notification of the threat through to cooperating with the RCMP. Although there have been some changes since the mid-2000s, these processes largely remain in place today.

Importantly, while the case of the Toronto 18 was seen as a huge success for Canada's counter-terrorism capabilities at the time, it also shaped expectations regarding how future threats would be treated. Canadian national security would spend much of the five to seven years after the Toronto 18 arrests looking for the next such group, a threat that never really manifested. In this way, the Toronto 18 may have contributed to bias in understanding an evolving national security threat that was manifesting in the form of lone actors and extremist travel.

* Stephanie Carvin is an Associate Professor at the Norman Paterson School of International Affairs, Carleton University. Her research interests are in the area of international and national security, and technology. She holds a PhD from the London School of Economics and published her thesis as *Prisoners of America's Wars: From the Early Republic to Guantanamo* (Columbia/Hurst, 2010). She is the author of *Stand on Guard: Reassessing Threats to Canada's National Security* (University of Toronto Press: 2021). She is also the author of *Science, Law, Liberalism and the American Way of Warfare: The Quest for Humanity in Conflict* (Cambridge, 2015), co-authored with Michael J. Williams. From 2012 to 2015, Dr. Carvin was an intelligence analyst with the Government of Canada, focusing on national security issues. The author is grateful to Mireille Seguin for her assistance in preparing background research for this chapter.

I. INTRODUCTION

Although the Toronto 18 case was not the first terrorism investigation the Canadian Security Intelligence Service (CSIS or “the Service”) managed in the post-9/11 era, it is certainly the most high-profile. And yet, little is publicly known about CSIS’s role in the case, relative to that of law enforcement agencies. To fill this gap, this chapter provides the first scholarly description of CSIS’s counterterrorism (CT) investigation process, the context in which it took place, and it assesses the impact of the case on the Service and the understanding of national security threats in Canada, generally. It argues that while the Toronto 18 case was a success for the Service, it represents something of a relic rather than being indicative of current CT threats. Moreover, it may have created certain biases within the organization, where the most pressing task was believed to be finding the next Al Qaida (AQ)-influenced terrorism “cell”, rather than how the threat itself was evolving or how new threats were emerging.

After a description of the Service’s role and its experience with CT prior to the Toronto 18, this chapter provides a broad outline of the Service’s CT investigative process that gives context in how it would have investigated the case. It then evaluates the legacy of the Toronto 18 case, as described above.

II. CSIS 101

The issue of terrorism (or violent extremism¹) has been extremely prominent in Canada since 9/11, but most Canadians remain unfamiliar with CSIS. A survey conducted by Ekos in 2018 found that only 30% of Canadians could name the government agency “that is responsible for investigating threats to Canada such as terrorism, espionage, and the proliferation of weapons of mass destruction.”²

¹ This chapter uses “terrorism” and “violent extremism” in an interchangeable way. The author’s preference is the latter term to cover acts of political violence which, for a variety of reasons, fall short of our legal definition of terrorism that nonetheless may meet the threshold for being a national security concern.

² Canadian Security Intelligence Service, *Attitudes to the Canadian Security Intelligence Services (CSIS): Base Line Study* (Report), by EKOS Research Associates, Catalogue No PS74-8/1-2018E-PDF (Ottawa: CSIS, 2018), <https://epe.lacbac.gc.ca/100/200/301/pwgsc-tpsgc/por-ef/canadian_security_intelligence_service/2018/report.pdf>.

Perhaps this should not be surprising for a security intelligence service that is often described as operating (as the cliché has it) “in the shadows.” Moreover, Canada has lagged behind other countries in terms of the review, oversight, and transparency of its national security services. Even those who have an interest in learning more about CSIS’s role in national security do not have many resources to work with. In this way, it is useful to begin this chapter with a brief outline of the Service’s role, not just for this chapter’s subsequent discussion of CSIS, but to place the organization and its role in context for the forthcoming chapters in Part II of this collection, which discuss CSIS and its relationship to the RCMP, its role in providing (or not providing) evidence at trial, and so on.

CSIS is Canada’s domestic national security intelligence service. It is mandated to collect information “within or relating to” threats to the security of Canada. These are defined in section 2 of the CSIS Act as espionage, foreign-influenced activities, terrorism (described as “activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state”) and subversion.³

As the Service is sometimes confused or conflated with similar organizations in allied countries, it is worth taking a moment to differentiate CSIS from its domestic and international counterparts. First, while the Service does operate overseas, it does so in relation to its mandate to collect information on threats to the security of Canada outlined in section 12 of the CSIS Act: “[i]f there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, the Service may take measures, within or outside Canada, to reduce the threat.” However, unlike most of its allies, Canada does not have a human foreign intelligence agency like the American Central Intelligence Agency (CIA) or British Secret Intelligence Service (SIS or MI6). Under section 16 of the CSIS Act, the Service may collect information on foreign states, groups of states, or individuals other than Canadian citizens or permanent residents, at the

³ Although “sabotage” remains in the CSIS Act, the Service ended its subversion investigations in 1986 due to the end of the Cold War and concerns over the surveillance of Canadians engaged in lawful activities, mostly by the RCMP. See Reg Whitaker, Gregory S. Kealey, and Andrew Parnaby, *Secret Service: Political Policing in Canada From the Fenians to Fortress America* (Toronto: University of Toronto Press, 2012), 395–96.

request of the Minister of National Defence or Foreign Affairs. However, this collection must take place within Canada.

Second, CSIS is primarily a human intelligence organization. That is, it employs and trains a cadre of intelligence officers (IOs) who engage with sources with whom they work in order to obtain information to support authorized investigations into threats to Canadian national security. This differentiates CSIS from Canada's signals intelligence agency, the Communications Security Establishment (CSE), which collects foreign intelligence through the global information infrastructure and defends Government of Canada systems and critical infrastructure designated by the Minister of National Defence under subsection 21(1) of the CSE Act. Importantly, the CSE is not permitted to collect information on Canadians, permanent residents, or anyone on Canadian territory. It may only do so under its mandate to assist federal law enforcement and security agencies (including CSIS), the Canadian Forces, and the Department of National Defence.

Third, the Service is a relatively small organization within the Canadian government. There are approximately 3,330 CSIS employees overall as of 2020, most of whom are located at the CSIS Headquarters in Ottawa, Ontario; there are also several regional offices throughout Canada. The Service has an annual budget of approximately \$570 million. By contrast, the Department of National Defence employs almost 95,000 (full-time) people and has an annual budget of approximately \$21.9 billion, while the RCMP employs over 30,000 people with an annual budget of approximately \$3.5 billion. Even the Toronto Police Service has approximately 7,900 employees and an almost \$1.1 billion annual budget. While all of these departments and agencies have roles beyond that of national security (making this an imperfect comparison), CSIS's relatively small budget is indicative of its narrow mandate relative to the other defence and law enforcement organizations listed above.

Fourth, unlike the above organizations, CSIS does not have the ability to arrest or detain individuals. While it may gather, store, and search information – and its IO have certain legislated powers to do so – it is a strictly civilian organization and may not cross into law-enforcement territory. Unless it is in extraordinary circumstances (such as engaging in its

lawfully mandated activities in a zone of conflict overseas⁴), its officers do not carry guns. However, as will be further discussed below, the Service does have some very strong powers it can wield, including the ability to engage in surveillance, run human-sources, and with the appropriate warrants, wiretap, and intercept communications of individuals the Service is targeting.

III. CSIS AND VIOLENT EXTREMISM BEFORE THE TORONTO 18

Prior to the creation of CSIS in 1984, CT operations in Canada were conducted by the Royal Canadian Mounted Police (RCMP). In the aftermath of the 1970 October Crisis, when the violent, nationalist *Front de libération du Québec* (FLQ) kidnapped a British diplomat and Quebec cabinet minister, the Mounties came under considerable pressure to ensure that such an incident was prevented from happening again. This pressure, combined with a lack of clearly defined procedures and regulations governing national security investigations, created a climate where RCMP officers engaged in a very aggressive series of tactics against targets perceived as being subversive or supportive of violent extremist movements.⁵ Once these tactics were exposed, they became known as the “dirty tricks campaign,” leading the (Pierre) Trudeau government to call for an inquiry into how the RCMP engaged in national security. The Royal Commission of Inquiry into Certain Activities of the RCMP (aka “The McDonald Commission”) would go on to make several recommendations, including the idea that the collection of national security information should be civilianized and separated from policing and criminal investigations. Heeding this advice, the Trudeau government established CSIS.

In the years after its creation, CSIS focused on a range of violent extremist activities, particularly “transnational” terrorism from conflict areas overseas that manifested into threat activity in Canada. This included Armenian terrorist attacks against Turkish targets in Canada, the Liberation Tigers of Tamil Eelam, and Sikh separatism (particularly the attack on Air India Flight 182 that killed 329 people). The failure to prevent this latter

⁴ This issue was controversial in relation to CSIS’s support to Canada’s mission in Afghanistan. See Colin Freeze, “Undercover CSIS Agents Carry Guns in Foreign Flashpoints,” *Globe and Mail*, May 25, 2010, <https://www.theglobeandmail.com/news/national/undercover-csis-agents-carry-guns-in-foreign-flashpoints/article4320423/>.

⁵ Whitaker, Kealey, and Parnaby, *Secret Service*, 271–364.

attack was, in part, due to a lack of proper cooperation between the Service (albeit in its first year of existence) and the RCMP and was a serious blight on the new organization.⁶ It also stood as a tragic reminder of what was at stake if Canada's national security agencies could not figure out how to work with each other on threats to the country.

By the 1990s, the Service had begun to monitor the rise of extremist networks motivated by religious extremism and their links to individuals in Canada. This included Shi'ite groups such as Hizballah, as well as Sunni groups like the Algerian Armed Islamic Group (GIA). The case of the "Millennium Bomber", Ahmed Ressay, was indicative of the threats that preoccupied national security departments and agencies after 2001. Ressay arrived in Canada on a false identity, travelled to the United States from Victoria, British Columbia, and planned to carry out a bomb attack against Los Angeles Airport on the eve of the Millennium. Ressay was caught by a U.S. border guard who noticed his nervousness as he attempted to enter from Canada.⁷

Therefore, although the Service had been aware of violent-extremist threats in Canada prior to 9/11, the aftermath of al-Qaeda's attacks on America still represented a dramatic change in how the Canadian government prioritized national security and intelligence. Being seen as a reliable CT partner for the United States and our allies became an issue of importance to the Jean Chrétien government, and they made a \$7.2 billion investment in the Canadian national security and intelligence community.⁸ They also created, for the first time, specific terrorism charges in the *Anti-Terrorism Act* (2001) and the first national security policy, *Securing An Open Society*, in 2004.⁹

⁶ There is no room in this chapter to discuss the impact of Air India 182 on CSIS or Canadian national security, generally. See Kim Bolan, *Loss of Faith: How the Air-India Bombers Got Away with Murder* (Toronto: McClelland & Stewart, 2005). See also Whitaker, Kealey, and Parnaby, *Secret Service*, 374–85.

⁷ Stewart Bell, *Cold Terror: How Canada Nurtures and Exports Terrorism Around the World* (Mississauga, ON: J. Wiley & Sons Canada, 2007) 161–70.

⁸ Greg Fyffe, "The Privy Council Office and the Canadian Intelligence Community," in *Top Secret Canada: Understanding the Canadian Intelligence and National Security Community*, eds. Stephanie Carvin, Thomas Juneau, and Craig Forcese (Toronto: University of Toronto Press, 2021).

⁹ Canada, Privy Council Office, *Securing an Open Society: Canada's National Security Policy*, Catalogue No CP22-77/2004E-PDF (Ottawa: Privy Council Office, 2004), <<http://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf>>.

For an agency like CSIS, which was used to low-levels of interest from other branches of government and previously avoided day-to-day policymaking in downtown Ottawa, the heightened attention on its activities and expectations to deliver in this new era meant added pressure on the organization.

Indeed, the demands to effectively combat terrorism and stay within a narrowly defined mandate consistently challenged the Service in the 2000s. For example, in 2007, CSIS was publicly reprimanded after its then-review agency – the Security Intelligence Review Committee (SIRC) – found that it likely overstepped its mandate, crossing over into law-enforcement activities by facilitating the handing over of Mohammed Mansour Jabarah, a Canadian and an admitted al-Qaeda member, to U.S. authorities. In addition, SIRC found that although Jabarah was a violent extremist, several of his *Charter* rights were violated and he was arbitrarily detained. SIRC made several recommendations regarding the handling of future cases.¹⁰

The Service also was criticized by courts and SIRC for destroying records. Previous Service practice (owing to its interpretation of the CSIS Act provisions that it can collect, analyze, and retain only that which is “strictly necessary”) was to destroy information after a period of time, so as to not keep files on Canadians forever. It was also criticized for endangering Canadians when discussing them with foreign officials and contributing to their mistreatment.¹¹ In this way, early terrorism cases proved to be something of a field of landmines for the Service as it tried to figure out where the (ill-defined) lines were while working at an unprecedented operational tempo. The main difficulty was that the Service had been given

¹⁰ Canada, Security and Intelligence Review Committee, *SIRC Annual Report 2006-2007: An Operational Review of the Canadian Security Intelligence Service*, Catalogue No PS105-2007E-PDF (Ottawa: SIRC, 2007), 18–22, <http://www.sirc-csars.gc.ca/pdfs/ar_2006-2007-eng.pdf>. For an overview of the Jabarah case, see Stewart Bell, *The Martyr's Oath: The Apprenticeship of a Homegrown Terrorist* (Mississauga, ON: J. Wiley & Sons Canada, 2005).

¹¹ On destroying records, see *Charkaoui v. Canada (Citizenship and Immigration)*, 2008 SCC 38. On the mistreatment of Canadians due to the actions of national security officials, see Canada, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar*, 3 vols (Kanata, ON: Gilmore Printing Services, 2006), <http://publications.gc.ca/collections/Collection/CP32-88-1-2006E-FB1.pdf>; *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin* (Kanata, ON: Gilmore Printing Services, 2008) (The Honourable Frank Iacobucci, Q.C.), <http://publications.gc.ca/collections/collection_2014/bcp-pco/CP32-902008-1-eng.pdf>.

more capacity to carry out its tasks, but it had not created up-to-date policies and guidelines for the new world it was now operating in, including an increased presence abroad.¹²

Of course, there were accomplishments too. The first successful terrorism charge in Canada was brought against Mohammed Momin Khawaja in 2004, and he was convicted in 2008 (later upheld by the Supreme Court).¹³ Khawaja had been part of a London-based cell and sought to facilitate bombmakers by designing a weapon, transferring funds, and recruiting individuals to assist in these efforts. The case proved to be a successful test of the new *Anti-Terrorism Act*, as well as the national security community's efforts to successfully prosecute a terrorism charge.

A. What CSIS Investigates

While the most pressing concern for CSIS employees working in CT is the threat of an armed attack within Canada (or a Canadian conducting an armed attack overseas), the Service monitors for other sorts of threat-related activity as well. This includes travel for extremist purposes (foreign fighters, called Canadian extremist travellers or CETs), financing and facilitating threat-related activity, and radicalization. In this sense, while CT investigations have at their core the goal of preventing extremist attacks, doing so requires monitoring a broad range of activities.

Indeed, it is likely that the majority of violent extremist activity in Canada is that which supports violent extremism, rather than direct attack planning. This is why statistics that highlight the fact that there are more people killed by moose or bathtubs than violent extremism are misleading. Non-violent activities that nevertheless support extremism cause disruption in communities, whether by furthering mistrust, siphoning funds from worthy charitable causes to extremist ones, and sowing division through the targeting of youths through radicalization and/or the intimidation of community members from speaking out.¹⁴ Worse, they may contribute to the killing and wounding of others overseas in attacks made possible by individuals providing support in Canada.

¹² Whitaker, Kealey, and Parnaby, *Secret Service*, 458.

¹³ *R v. Khawaja*, 2012 SCC 69.

¹⁴ Canada Centre for Community Engagement and the Prevention of Violence, *National Strategy on Countering Radicalization to Violence*, Catalogue No. PS4-248/2018E-PDF (Ottawa: Government of Canada, 2018), 13-14, <<https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-strtg-cntrng/ntnl-strtg-cntrng-rdclztn-vlnc-en.pdf>>.

B. How CSIS Investigates Violent Extremism

Whatever the form of violent extremism, the Service’s investigations typically begin through a “tip,” either from the public or through a foreign government that has information to suggest that someone within Canada may be engaging in threat-related activity. In addition, it is common that the Service may find out about an individual through their connections to other individuals who are under investigation. This section provides a general description of how CT investigations proceed, with a view to providing some insight into how the Toronto 18 investigation likely took place.

The Service has a considerable range of authorities it can use when it becomes aware of a potential threat to national security. The most important of these is the ability to “target” an individual, person, organization, or event suspected of constituting a threat to the security of Canada. Targeting activities are governed by the rules and procedures set out in the CSIS Act, ministerial directives, Service policy, and other related procedures.¹⁵ In using them, the Service must follow the rule of law, the means employed must be proportional to the gravity and the imminence of the threat, they must use the least intrusive techniques first (except for emergency situations), and the level of authority required must “be commensurate with their intrusiveness and risks associated with using them.”¹⁶ All targeting decisions are provided to senior CSIS personnel (typically an assistant director or assistant deputy minister-level managers) within a five-day period from the date of approval.¹⁷ CSIS procedures state that regional director generals (RDGs) are to consult with the director generals of the appropriate headquarters branch on all targeting decisions to ensure consistency and coordination.¹⁸

¹⁵ CSIS, *Internal Audit of Operational Compliance: Targeting*, (880-144), March 2013. Documents available through ATIP by the Globe and Mail. See Colin Freeze, “CSIS Documents Reveal how Agency Designates Terrorism Targets,” *Globe and Mail*, February 11, 2015, <https://www.theglobeandmail.com/news/politics/csis-documents-reveal-how-agency-designates-terrorism-targets/article22905797/>.

¹⁶ CSIS, *Internal Audit*, 1.

¹⁷ CSIS, *Internal Audit*, 1.

¹⁸ Who is in charge of this investigation depends on its location. As noted above, the Service is represented across Canada in several regional offices. In the case of the Toronto 18, the suspects were located in the Greater Toronto Area (GTA), and the Toronto Regional Branch (TR) was given the lead responsibility. However, regions will stay in touch with headquarters, normally through the “desk” assigned to a particular threat or region.

Targeting authorities themselves are broken up into two main categories: those for when investigators have reason to suspect an individual may be engaged in threat-related activity and those for when the Service believes it can demonstrate to a federal judge that it believes an individual is engaged in threat-related activity, and more powerful investigative tools are required.

The former set of authorities are governed within the Service and typically require the support of a director general (DG) to authorize. The authorities are divided up into different investigative levels. During the Toronto 18 investigations, there were three levels: Level 1, which allowed for basic information gathering, moving up through to Level 3, which allowed for more intrusive means, including physical surveillance. (Today, CSIS has simplified this into two levels 1 and 2.) According to CSIS documents released under the Access to Information and Privacy (ATIP) policy, several factors are taken into account when selecting the appropriate targeting level, including the nature, imminence, and significance of the threat, the collection techniques allowed, and the availability of resources to conduct the investigation.¹⁹

Once the Service moves from “suspecting” individuals might be engaged in threat-related activities to the point where they “believe” that they are doing so, and they feel the need to use more intrusive means to gather information, they can appeal to the Federal Court for a warrant under section 21 of the CSIS Act. The warrant is necessary under the *Canadian Charter of Rights and Freedoms* to protect individuals from unreasonable search and seizure. Court documents indicate that, during the Toronto 18 investigation, CSIS was engaging in electronic surveillance during its investigation.²⁰

The process to obtain a warrant is far from a rubber stamp process; applications may often run more than 50 pages, and every line must be supported (typically described as “facted” within Service jargon) with evidence. Government of Canada lawyers vet the applications rigorously, and they are subject to several layers of management approval. In addition, Service personnel are often required to testify to the information in the warrant and answer any questions federal judges may apply. In this sense, drafting warrants may take several months.

¹⁹ CSIS, *Internal Audit*, 4.

²⁰ See the decision in *R v. Ahmad*, 2009 CanLII 84779 at para 11 (ON SC) [*Ahmad* ONSC].

The reason for this diligence is clear: judges can be very demanding of the Service if they feel any information provided in the warrant application is missing, misleading, or unsupported. If judges feel that the Service has not met its “duty of candor,” they will deny or even revoke warrants that have been issued.²¹ Nevertheless, the system can move quickly if needed. In the wake of a serious incident, the Service can apply for warrants to conduct investigations in order to ensure the safety of Canadians. But for a relatively slow investigation such as the Toronto 18, the full warrant process was required.²²

As noted above, CSIS is a human intelligence agency where IOs collect information in support of national security investigations. This can be done in a variety of ways. IOs may begin by simply performing a basic internet search and speaking to friends and relatives or even the targets themselves. IOs have been known to show up to the workplaces of the individuals they wish to speak with – a practice that has been controversial and the subject of several complaints of harassment and intimidation.²³ However, IOs do not have the freedom to speak with whomever they please. Investigations normally follow a plan, requiring layers of approval. Further, additional and

²¹ In X(Re), 2014 FCA 249, the Federal Court of Appeal found that the Service had violated its duty of candour to the Court in seeking a warrant for surveillance. See Maciej Lipinski, “X(Re): A Check on CSIS Powers or a Roadmap for Expanding Them?,” *theCourt.ca*, November 6, 2014, <http://www.thecourt.ca/xre-a-check-on-csis-powers-or-a-roadmap-for-expanding-them/>. This issue came into the public eye once more in July 2020, when a Federal Court ruling that CSIS had repeatedly violated its duty of candour up until 2019 – the third time such a ruling had been made since 2013. For more on this issue, see Leah West, “Secret law used by security establishment threatens public trust,” *Policy Options*, July 22, 2020, <https://policyoptions.irpp.org/magazines/july-2020/secret-law-used-by-security-establishment-threatens-public-trust/>. The Service appealed this decision in October 2020.

²² Alternatively, in threat to life scenarios (such as the knowledge that an individual under investigation has access to a weapon and the intent to use it), the Service may inform the RCMP or other police service of an incident in order to prevent serious harm from occurring. While such an intervention may harm an investigation, the serious risk of a loss of life will trump operational concerns.

²³ See Shanifa Nasser, “When CSIS Comes Knocking: Amid Reports of Muslim Students Contacted by Spy Agency, Hotline Aims to Help,” *CBC News*, August 7, 2019, <https://www.cbc.ca/news/canada/toronto/csis-students-university-muslim-campus-1.5229670>. Of note, most of the complaints date to 2012–2013. CSIS continues to speak with individuals in communities as a part of their lawful investigations and says it has changed some of its practices in this regard. Still, it is clear that there are those who believe that these visits damage community relations and that it continues to create mistrust with marginalized communities.

specific permissions and authorities are required from regional DGs for “sensitive sectors,” such as educational and religious institutions. All of this is done to ensure that investigations keep within the letter and the spirit of the law but also to anticipate and manage blowback from individuals and the community who may feel unduly targeted. More will be said on this below in relation to the Toronto 18 investigation.

IOs are also trained to recruit sources that can provide information to investigators to support the investigation. While most interactions IOs will engage in during an investigation are casual, in some cases the relationship may become formalized over time. In these cases, individuals who may be motivated by patriotism, a sense of adventure, money, or all of the above, are tasked with gathering information to assist the investigation.

Supporting the work of the IOs is a network of individuals within the regional branches as well as headquarters. Each region has a Physical Surveillance Unit (PSU) that sends out teams of individuals who help to establish the patterns of life and observe the behaviours of individuals under investigation. This information assists IOs in learning, for example, who a target is in regular contact with and to identify if they are deviating from their regular habits in such a way that may identify they are engaged in threat-related activity.

Within the Service, there are also a number of analysts assisting the investigation in several ways. Helping IOs make sense of a case are tactical analysts that are often embedded in regional desks. These analysts take disparate pieces of information and clarify networks, establish timelines, and assist in identifying key individuals within a larger target set. Additionally, whereas IOs are typically rotated to different desks every two to five years, these analysts tend to stay in their roles, becoming “institutional memory”, particularly on longer-term investigations. Communications analysts translate and interpret information gathered (usually under warrant) but are also able to get to know and understand targets from listening, observing, and reading their interactions. Finally, strategic analysts help to contextualize the investigation within a bigger picture. For example, with CT investigations, strategic analysts can provide insight on the kinds of materials a target is consuming and how observed behaviour fits known patterns of mobilization to violence, generally.

Finally, there are units within the Service that provide technical expertise (such as providing scientific analyses of the kinds of bomb-making materials a target may be trying to acquire), open-source information (using

research librarians at the Service's Information Centre), and legal support from Government of Canada lawyers through the duration of the investigation. All of these can play key roles in ensuring that an unpredictable investigation runs as smoothly as possible.

Once an investigation is up and running, it may go in a number of ways. Individuals who appear to be mobilizing to violence may gradually (or even suddenly) change course with their plans. It is not unusual for individuals that appear to be highly motivated to engage in threat-related activity to suddenly disengage from it. For example, individuals who had been struggling to find work may find employment. Other individuals may become distracted by the mundane activities of everyday life, such as trying to raise and support a family. In other cases, loved ones may successfully intervene, or the individual may grow disillusioned with extremist messaging. While not necessarily a Service success specifically, disengagement is undoubtedly a positive outcome.

However, a challenge for IOs is that Service targets often go through different phases in their willingness or capacity to mobilize to violence; the path a target takes is often anything but linear. In this way, periods of disengagement may be followed by a sudden return to supporting violent extremism or even mobilization, and this may be followed by a gradual withdrawal once again. Following this cycle may take months or even years. If, in the course of the investigation, the Service comes to the point where it believes that the targets are engaging or about to engage in criminal activity, they alert the RCMP who then proceed to begin a criminal investigation based on a "disclosure letter" from the Service. How this works in practice will be discussed below with reference to the Toronto 18 case.

IV. CSIS AND THE TORONTO 18 INVESTIGATION

As noted above, there is not much in the way of publicly available information on CSIS's role in the Toronto 18 case. Nevertheless, the available but fragmentary information about its activities in this case paints a picture that is consistent with the account described above.

CSIS's involvement in the Toronto 18 case may date back as far as 2002 when the Service began to watch eventual ringleader Fahim Ahmad's activities on the internet as he chatted with like-minded individuals on

extremist forums.²⁴ However, the investigation into what became known as the Toronto 18 cell appears to have picked up steam sometime around 2004–2005, when a group of individuals, including Ahmad, appeared to be engaged in radicalization activities.²⁵

Interestingly, it appears that the Service tried to stop the group before it went too far down the path of mobilization. According to the journalist Stewart Bell, “CSIS initially tried to break the group with a disruption campaign” that involved CSIS officers approaching cell members and their parents, informing them they were on the Service’s radar. However, this appears to have had very little effect on the plotters, who continued their plans.²⁶ In 2010, not long after the Toronto 18 investigation concluded, SIRC raised concerns that these disruptions potentially went beyond the Service’s mandate and that the government should monitor them closely.²⁷

In the wake of the failed disruptions, CSIS continued to monitor Ahmad. It was soon discovered that he rented a car for two individuals, Yasin Mohammed and Ali Dirie, in August 2005. Mohammed and Dirie subsequently drove to the United States in a two-week effort to procure guns. Upon their return, the two were arrested for gun smuggling at the Peace Bridge as they attempted to return to Canada – their arrests due to the fact that they were on the authority’s radar.²⁸

As it became apparent that these individuals may be mobilizing to violence, the Service was able to recruit a source to infiltrate the cell in an

²⁴ Michelle Shephard, *Decade of Fear: Reporting from Terrorism’s Grey Zone* (Vancouver: Douglas & McIntyre, 2011), 115.

²⁵ Bell, *Cold Terror*, 252.

²⁶ Bell, *Cold Terror*, 254. See also Shephard, *Decade of Fear*, 116. Of note, civil liberties groups such as the National Council of Canadian Muslims, have expressed concerns about the use of CSIS’s threat disruption measures. Ihsaan Gardee, “Government Must Rebuild Trust with Canadian Muslims on National Security,” *The Hill Times*, June 11, 2018, <https://www.nccm.ca/government-must-rebuild-trust-with-canadian-muslims-on-national-security/>.

²⁷ Canada, Security Intelligence Review Committee, *Annual Report 2009-2010*, Catalogue No. PS105-2010E-PDF (Ottawa: SIRC, 2010), 16, <http://www.sirccsars.gc.ca/pdfs/ar_2009-2010-eng.pdf>. After being granted sweeping “threat reduction” powers in 2015 under the Harper Government’s Bill C-59, the Trudeau government kept “disruption” as a national security tool for the Service but defined it within narrow parameters in Section 21 of the CSIS Act. A critique of disruption powers (as they existed in Bill C-51) can be found in Craig Forcese and Kent Roach, *False Security: The Radicalization of Canadian Anti-Terrorism* (Toronto: Irwin Law, 2015), 225–70.

²⁸ Bell, *Cold Terror*, 255; Shephard, *Decade of Fear*, 107.

investigation that soon became known as “Operation Claymore.” It also played a role in securing the recruitment of a second individual who convinced the cell that he could procure explosives for them.²⁹ Open source and court reporting suggest that this second source was already “under development” as an informant for the Service between February and April 2006.³⁰

A decision to alert the RCMP, who could engage in a criminal investigation of the case, was made, and the official handover was in November 2005. This was done with the exchange of a “disclosure letter” from CSIS which indicated that Fahim Ahmad was believed to be engaging in activities that pose a threat to the security of Canada.

However, this was not the end of CSIS’s investigation into the Toronto 18 case. Following the handover, CSIS established a parallel investigation, not for the purpose of obtaining evidence or contributing to the RCMP investigation, but, in the words of the Ontario Superior Court, “in order to fulfill its mandate under s. 12 of the *Canadian Security Intelligence Service Act*.”³¹ As such, CSIS members worked with the RCMP but for the purpose of ensuring that information flowed back to the Service rather than helping inform the federal police force.³² During the RCMP investigation, CSIS handed over further information in several “disclosure” and “advisory” letters (carefully crafted and vetted letters from CSIS to the RCMP containing intelligence and permitting its use in legal proceedings). The basic information in these letters was used by the RCMP to obtain warrants that were then used in the investigation.³³

V. SIGNIFICANCE AND LEGACY

The Toronto 18 investigation was, and remains, significant for CSIS for a number of reasons. One of the reasons may be the fact that, according to media coverage, CSIS’s regional office in Toronto was a target of the cell – making it the first time CSIS employees were themselves at the centre of a plot.

²⁹ Bell, *Cold Terror*, 254; Shephard, *Decade of Fear*, 115.

³⁰ Michael Friscolanti, “The Four-Million Dollar Rat,” *Macleans*, February 7, 2007, <https://archive.macleans.ca>; *Ahmad* ONSC, CanLII at para 63.

³¹ *Ahmad* ONSC, CanLII at para 7.

³² *Ahmad* ONSC, CanLII at para 44.

³³ *Ahmad* ONSC, CanLII at para 39.

However, the high-profile case had an impact on Service investigations for the next decade and a half in at least four ways. First, the Toronto 18 case was the largest and most important post-2001 counterterrorism operation in Canada, and it was a success. It was proof that the Service could handle a major investigation of a threat to Canadian national security in a new era of violent extremism. In addition, the courts upheld CSIS's practices in relation to "intelligence-to-evidence" with the RCMP, even if problems in that area remain. This meant that the amount of CSIS information that was brought to trial was minimized, protecting the Service's sources and methods.

A second significance is in what the Toronto 18 represented in the mid-2000s: the threat of terrorism was shifting from threats coming to Canada from abroad to "homegrown" violent extremism. In other words, terrorist threats to Canada were coming from individuals who had been born in Canada or who had spent the vast majority of their lives within its borders. While there would still be plots that originated overseas (such as the 2006 Transatlantic Airline Plot), most Service investigations largely focused on Canada-based extremists.

A third significance is the legacy of the Toronto 18 case in terms of the biases it may have created. The nature of the Toronto 18 case is a classic "left-of-bang" scenario - over several months, a number of individuals are observed engaging in threat-related activity, a Service investigation is mounted which then becomes an RCMP investigation that leads to an arrest disrupting a plot before an attack is carried out. Therefore, in the same way that armies often prepare to fight the last war, a question could be raised as to whether or not the Canadian national security community, including CSIS, spent its time and resources looking for the next "Toronto 18" rather than thinking about how violent extremism in Canada would evolve over the next decade.

While there were other domestic cells that were disrupted in Ottawa (2009) and Toronto (2013), within six years of the Toronto 18 case, violent extremists in Canada began to mobilize to violence by travelling overseas to war zones, especially Syria, rather than plotting attacks at home. Indeed, there were signs this was taking place as early as 2009 when six Canadians from Toronto left to travel to join Al Shabaab in Somalia.³⁴ Eventually,

³⁴ Stewart Bell, "Canadian Appears in Terror Group's Propaganda Video Two Years after Being Killed in Somalia," *National Post*, January 8, 2015, <https://nationalpost.com/new/s/canadian-appears-in-terror-groups-propaganda-video-killed-in-somolia>.

more would follow them in travelling to East Africa as well as South Asia over the next several years, but this general trend appears to have gone generally unnoticed until 2014.³⁵

Of course, it goes without saying that prediction is difficult, and anticipating how threat of violent extremism will evolve is extremely challenging. How could an analyst working on the Toronto 18 case have reasonably anticipated that a mass uprising in the Arab world in late 2011 would unleash a massive civil war that would revitalize al-Qaeda in Iraq (now Daesh) and draw in tens of thousands of extremist travellers? Moreover, Canada was not alone in failing to anticipate the rise of extremist travellers as a major national security threat of the 2010s. Still, a bias towards looking for the next domestic “cell” may have prevented the Service (institutionally) from seeing this shift earlier as it was looking for more of what had already happened rather than trying to figure out what may happen next.

A final significance of the Toronto 18 case is more of a reflection as to how much has changed since 2006. Today, while Al Qaida/Daesh-inspired extremism remains a concern, the Service now actively investigates a broader range of violent extremism, including religiously-, ideologically-, and politically motivated causes. Indeed, the deadliest attacks to occur in Canada since 9/11 have been carried out by individuals with racist/xenophobic/anti-immigrant or misogynist views. Moreover, rather than violent extremist “cells”, successful attacks have been perpetrated by lone actors who appear to have mobilized to violence quickly. This includes the 2014 attacks in Saint-Jean-sur-Richelieu and Ottawa, as well as the 2017 Quebec City mosque shooting and the 2018 Toronto van attack.

Moreover, it is clear that CSIS is now re-evaluating the emphasis that has been placed on violent extremism generally in the last two decades. In its 2019 Public Report, the director described geo-economic threats (such as economic espionage) as “the greatest danger to Canada’s national security” – a significant change from prior reports.³⁶ This suggests a recognition that

³⁵ By 2011 it was estimated that up to 20 Canadian youths had travelled to Somalia to join Al Shabaab. See “Somali Militant Group Recruiting Canadian Youth,” *CBC News*, January 26, 2011, <https://www.cbc.ca/news/canada/somali-militant-group-recruiting-canadian-youth-1.1052143>; “Terror Charges Laid Against Former Winnipeggers,” *CBC News*, March 15, 2011, <https://www.cbc.ca/news/canada/manitoba/terror-charges-laid-against-former-winnipeggers-1.1015496>.

³⁶ Canadian Security Intelligence Service, *CSIS Public Report 2019* (Ottawa: Public Works and Government Services Canada, 2020), 4, <<https://www.canada.ca/content/dam/cs-is-scrcs/documents/publications/PubRep-2019-E.pdf>>.

long-term campaigns aimed at either strategically undermining or skewing the landscape of the Canadian economy pose a greater threat to the well-being of Canada than the threat of violent extremism.

In this sense, while the Toronto 18 case can be considered a success for the Service, it is also something of a historical artifact. The nature of the threat of violent extremism and national security threats in Canada have evolved in a decade and a half. CSIS has had to adjust along with other national security agencies. The best lesson to take from this case is to use it as a benchmark to observe the shifts and changing threats the Service has had to face and will face in the future.

This, however, has not been easy. A decade and a half's worth of focusing on CT at the expense of counterintelligence (CI) means that there is much work to do. Indeed, the neglect of CI issues means that key Canadian institutions – including the national security and intelligence community, the courts, political bodies, and the public – arguably lack knowledge and/or experience with these issues. The result is that Canada is arguably less prepared for what will likely be the main security challenges for the next decades of the 21st Century. In this sense, the Toronto 18 case should be considered a past success for CSIS but also a warning about the myopias that can be generated in the national security space.