Canadian Security Intelligence Service (CSIS)
and
Integrated Terrorism Assessment Centre (ITAC)
Institutional Report Prepared for the Public Order Emergency Commission

Contents

1. Department overview

1.1. CSIS mandate and organizational and reporting structure

Statutory mandate

Established in 1984, the Canadian Security Intelligence Service (CSIS or the Service) is a civilian security intelligence service. CSIS' core mandate is to investigate threats to the security of Canada and advise the Government of Canada on such threats. The *Canadian Security Intelligence Service Act (CSIS Act)* identifies the specific activities that the Service may investigate as well as the threshold that must be met for CSIS to engage in investigative activities.

Pursuant to s. 12 of the *CSIS Act*, CSIS "shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada." Section 2[1] of the *CSIS Act* defines "threats to the security of Canada"; they are commonly understood as:

- (a) espionage and sabotage;
- (b) foreign-influenced activities (or foreign interference);
- (c) terrorism and violent extremism; and
- (d) subversion.

Section 2 further specifies that "threats to the security of Canada" "does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d)."

In addition to its mandate to investigate threats to the security of Canada, CSIS also has the authority under s. 12.1 of the *CSIS Act* to take measures to reduce these threats in certain circumstances. The Act identifies the parameters that must be met to exercise this authority, as well as certain prohibited activities.

Beyond the s. 12 mandate, the *CSIS Act* provides other duties and functions. Specifically, s. 13 authorizes CSIS to provide security assessments on individuals who require access to classified information or sensitive sites within the Government of Canada. Section 14 authorizes CSIS to provide security advice relevant to the exercise of a power or performance of a duty or function under the *Citizenship Act or the*

[1] [1] The complete definition of "threats to the security of Canada" in s. 2 of the *CSIS Act* is:

> (a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,
> (b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,
> (c) 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
> (d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada,

but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).

Immigration and Refugee Protection Act. Pursuant to s. 15, CSIS may conduct such investigations as are required for the purposes of providing the aforementioned security assessments or security advice.

Finally, pursuant to s. 16, CSIS may collect foreign intelligence, within Canada, at the request of the Minister of Foreign Affairs or the Minister of National Defence and with the consent of the Minister of Public Safety.

Reporting structure

Pursuant to s. 6 of the *CSIS Act*, the "Director, under the direction of the Minister, has the control and management of the Service and all matters connected therewith." The responsible minister is the Minister of Public Safety. Supporting the Director in his management of the Service are three Deputy Directors representing Operations, Policy, and Administration, and five Assistant Directors.

The Deputy Director Operations (DDO) heads the operations directorate that is responsible for the operational activities of the Service. The DDO reports to the Director and is responsible for several program areas, including collection, assessments, threat reduction and security screening.

The DDO is supported by two Assistant Directors. The Assistant Director Collection (ADC) manages and oversees all operational collection activities, both foreign and domestic. The Assistant Director Requirements (ADR) supports the DDO with the overall management of the Service's operational and analytic activities from National Headquarters.

The Deputy Director of Policy and Strategic Partnerships (DDP) supports the Director by developing and providing strategic policy advice to the Director as well as managing the Service's strategic partnerships with external stakeholders.

The Deputy Director Administration (DDA), who is the Service's Chief Financial Officer (CFO), provides strategic advice on expenditures and responsible stewardship and financial management. Reporting to the Director, the Assistant Director Human Resources (ADH) is responsible for all human resource matters, including recruitment and staff, learning and development, and health and workplace management.

Also reporting to the Director, the Assistant Director Technology (ADT) is responsible for all facets of the Service's technological requirements, both corporate and operational.

In June 2022, the position of Chief Transformation Officer (CTO) was created, reporting to the Director. The CTO leads the Transformation Hub, charged with centralizing and organizing efforts to plan for the future and implement transformational programs, and seeks to ensure that within an increasingly data-driven world shaped by technology, CSIS continues to be able to deliver on its mandate to Canadians.

The National Security Litigation Advisory Group (NSLAG), which is staffed by DOJ lawyers who do not come under the direction of CSIS managers, provides legal services to CSIS. The Assistant Director Legal Services (ADL), a Senior General Counsel from the Department of Justice (DOJ), oversees NSLAG.

1.2. ITAC organizational structure and reporting structure

The Integrated Terrorism Assessment Centre (ITAC), created out of the Government of Canada's 2004 national security policy "Securing an Open Society," was established to independently produce comprehensive threat assessments using a wide range of classified and unclassified sources. ITAC is intended to serve as a "community resource" in supporting government decision-making and providing timely analysis to security partners.

ITAC has three main program areas:

- Assessing and reporting on terrorism threats, trends and events;
- Assessing and recommending the National Terrorism Threat Level (NTTL) for Canada;
- Assessing and setting terrorism threat levels for Canadian interests worldwide, including for special events and internationally protected persons.[2]

ITAC develops threat assessments using classified reporting, information shared by security partners and openly available information. The threat level methodology evaluates threat actors' intent, capability and opportunity to conduct an act of terrorism. The methodology takes into account known mitigation measures by police and other security partners. ITAC's assessments represent the threat level at a point in time. While assessments may include projections, they must be regularly updated to account for changes in the security environment and new reporting. For this reason, ITAC is regularly re-evaluating threat levels.

ITAC is solely an assessment body. It does not collect intelligence. Instead, ITAC relies on intelligence collected by domestic and international partners, including CSIS, and openly available information to produce its threat assessments.

ITAC is collocated with CSIS and operates under the provisions and authorities of the *CSIS Act*. It is also subject to Ministerial Directions issued by the Minister of Public Safety to CSIS, as well as internal CSIS policies and procedures.

The Executive Director of ITAC works under the authority of the Director of CSIS, in consultation with the National Security and Intelligence Advisor (NSIA).[3] The NSIA chairs the Deputy Ministers' Committee on National Security (DMNS), which has a role in reviewing ITAC's performance and providing advice on its strategic direction. Every year, ITAC submits an annual report to DMNS. Departments and agencies represented at DMNS fund a portion of ITAC's budget through a Memorandum of Understanding that is renewed every five years.

Reporting to the Executive Director of ITAC are the Director General of Assessment, who leads a team of intelligences analysts, and the Director General of Policy and Partnerships, who is responsible for external engagements, dissemination and corporate support.

[2] https://www.canada.ca/en/security-intelligence-service/integrated-terrorism-assessment-centre.html

[3] ibid

1.3. Legal framework for CSIS information and intelligence collection

As stated above, CSIS' authority to collect information and intelligence on threats to the security of Canada rests primarily in s. 12 of the *CSIS Act*. Section 2 defines "threats to the security of Canada." In particular, s. 2(c), which is commonly referred to as terrorism and violent extremism, reads: "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."

CSIS's statutory authority to collect information and intelligence on s. 2(c) threats is predicated on two conditions:

1. Meeting the threshold of "reasonable grounds to suspect" that the activities constitute 2(c) threats; and
2. Restricting the information and intelligence collection to what is "strictly necessary".

The "strictly necessary" condition limits the Service's collection and retention of information to only that which is required fulfill its national security mandate. To ensure an effective, compliant and rigorous institutional approach to the strictly necessary requirement, the Service has developed operational guidance for employees on how to apply a principled approach to their collection and retention decisions. The Service's decisions to collect and retain information further to its core mandate must be: reasonable; justified; and accountable. The principles set out the Service's interpretation of this key concept in CSIS' core authority, ensuring a consistent understanding and application of the strictly necessary requirement in line with CSIS' legal authorities, the rule of law and the *Charter*.

Where CSIS' collection activities do not interfere with an individual's reasonable expectation of privacy as defined in Canadian jurisprudence (the totality of circumstances test), s. 8 of the *Canadian Charter of Rights and Freedom* is not engaged and CSIS' investigation need only comply with the statutory conditions of s. 12 of the *CSIS Act*. Where CSIS' collection activity does encroach on a person's reasonable expectation of privacy, the Federal Court has recognised that s. 12 of the *CSIS Act* can lawfully and reasonably authorise CSIS to conduct warrantless searches and seizures that are no more than minimally intrusive of protected privacy interests[4] and are carried out in a reasonable manner[5].

Any collection activity by CSIS that intrudes more than minimally on a person's reasonable expectation of privacy must be judicially authorised by a warrant issued by the Federal Court pursuant to s. 21 of the *CSIS Act*. Under that provision, following an application made in writing, a designated judge of the Federal Court may issue a warrant if satisfied that CSIS has demonstrated that there are "reasonable grounds to believe" that the warrant is required to enable the Service to investigate the threat. Section 21 warrants enabling CSIS to investigate threats to the security of Canada, including 2(c) threats, are issued for a maximum period of one year.

[4] Mahjoub (Re), 2013 FC 1096, confirmed in Mahjoub v Canada (Citizenship and Immigration), 2017 FCA 157, leave to appeal to the Supreme Court of Canada denied (17 May 2018); X (Re), 2017 FC 1047; CSIS Act (CA) (Re), 2020 FC 697.

[5] To comply with the third general condition originally set out in R v Collins, [1987] 1 SCR 265, for a warrantless search to be reasonable and thus compliant with section 8 of the Charter. On this point, see also R v Genest, [1989] 1 SCR 59.

Aside from section 12, the dataset regime in the *CSIS Act* (ss. 11.01 to 11.25) authorises CSIS to collect datasets containing personal information not directly and immediately related to activities that represent a threat to the security of Canada but are nevertheless relevant to the performance of CSIS' duties and functions under sections 12 to 16. "Dataset" is defined under s. 2 of the *CSIS Act* as "a collection of information stored as an electronic record and characterised by a common subject matter." CSIS' collection of datasets under the dataset regime does not require a warrant. However, for CSIS to be lawfully authorised to retain the dataset, either judicial or ministerial authorisation is required and CSIS must request such authorisation within 90 days of collection.

Where the dataset concerns predominantly Canadians or individuals within Canada ("Canadian dataset"), *judicial authorisation* is required for its retention and is valid for up to two years. Notably, before CSIS collects a Canadian dataset, there must first be an approved class for it.[6] Where the dataset predominantly relates to non-Canadians who are outside Canada ("foreign dataset"), a *ministerial authorisation* is required for its retention and is valid for up to five years. CSIS requires no authorisation to retain datasets of information publicly available at the time of collection ("publicly available collection"). Although hacked and leaked datasets technically make information available in the public domain, CSIS has committed before Parliament to treat such datasets as foreign or Canadian, not publicly available, and therefore their retention requires ministerial or judicial authorisation.

In addition to the *Charter*, *CSIS Act* and other applicable statutes, operational activities, including collection, are also subject to Ministerial Directions issued pursuant to s. 6(2) of the *CSIS Act*. This includes the 2015 Ministerial Direction for Operations and Accountability and the 2019 Ministerial Direction for Accountability. Additionally, CSIS is guided by Government of Canada directions pursuant to the *Avoiding Complicity in Mistreatment by Foreign Entities Act*. CSIS also has a suite of policies and procedures specific to operational activities. These policies and procedures are guided by the CSIS Policy Framework, which identifies as fundamental principles that every activity the Services conducts will be lawful and authorized, necessary, proportionate, and represent an effective and efficient use of public resources.

1.4. Targeting authority

All CSIS operations must be lawful and authorized, necessary, proportionate, and represent an effective and efficient use of public resources.

CSIS can open an investigation on an individual, a group of persons or an organization whose activities are reasonably suspected of constituting a threat to the security of Canada as defined under the *CSIS Act* and who is the subject of an authorized targeting level. CSIS may also target issues or events to allow for an investigation of activities which are reasonably suspected of constituting a threat to the security of Canada that arise because of, or are related to, the issue or event (eg. Threats to Vancouver 2010 Olympics).

[6] At least once a year, the Minister of Public Safety must determine classes of Canadian datasets for which collection is authorised, based on whether such collection is relevant to the performance of CSIS' duties and functions under sections 12, 12.1 and 16 of the CSIS Act, and the Intelligence Commissioner must review and approve these classes: see section 11.03 of the CSIS Act and section 16 of the Intelligence Commissioner Act.

Investigative authorities are reviewed by multiple levels of CSIS management before they are approved, and highly sensitive investigations may require senior executive approval.

All of CSIS' activities are subject to review by National Security and Intelligence Review Agency and the National Security and Intelligence Committee of Parliamentarians.

1.5. Definition of section 2(c) threats: terrorism, violent extremism and acts of serious violence

As mentioned above, section 2 of the *CSIS Act* defines threats to the security of Canada as espionage and sabotage, foreign-influenced activities, terrorism and violent extremism, and subversion.

The definition of "threats to the security of Canada" specifically excludes lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities constituting threats to the security of Canada.

Section 2(c) of the CSIS Act states that one of the threats to the security of Canada can be defined as

> *"activities within or relating to Canada directed towards 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"*

Based on this definition, CSIS can investigate politically, religiously and ideologically motivated violent extremism (PMVE, RMVE, and IMVE in short). Since 2019, CSIS has led various Government of Canada initiatives to better define, categorize and understand IMVE in Canada. In 2021, CSIS released a detailed placemat outlining the methodology used to assess when an activity reaches a national security threshold in relation to s. 2(c) of the *CSIS Act* (as opposed to constituting only a criminal activity or the exercise of free speech).

The placemat explains the steps CSIS takes to ascertain whether an identified IMVE threat actor represents a section 2c threat. An actor must meet three criteria;

a) show a willingness to kill or inspire others to kill,
b) show a desire or attempt to affect societal change, and
c) show an ideological influence.

If an actor only demonstrates an attempt to affect societal change and has an ideological influence, they may still be considered a 2(c) threat if there is a threat of serious violence.

1.6. Definition of section 2(d) threats: subversion

Section 2(d) of the *CSIS Act* defines a threat to the security of Canada as:

> *"activities directed toward undermining by covert unlawful acts, or directed towards or intended ultimately to lead to the destruction or overthrow by violence of the constitutionally established system of government in Canada"*

This threat is commonly referred to as subversion. For a threat to be considered subversion, it must be covert and illegal in nature, or exhibiting serious violence, for the purpose of undermining or destroying the constitutionally established system of government in Canada.

1.7. The IMVE threat landscape prior to the Convoy

IMVE is a serious threat to the security of Canada. Since 2014, Canadian ideologically motivated violent extremists have killed 25 people and wounded 41others in Canada.

The IMVE threat landscape in Canada is fluid and rapidly evolving. CSIS observed that the motivations behind IMVE were becoming more complex. Individuals are no longer influenced by a singular and definable belief system, but rather by a range of very personal and diverse grievances including conspiracy theories, from across the traditional left/right wing ideological spectrum. The resulting worldview often consists of personalized narratives that centre on the willingness to incite, enable and/or mobilize to violence.

For that reason, CSIS took a leading role in developing an understanding and terminology that more accurately depicts the broad range of motivations behind this particular extremist threat facing Canada. Based on its findings, CSIS decided to stop using the terms "right-wing" and "left-wing" to define the threat. Instead, it uses ideologically motivated violent extremism or IMVE – a term that has been adopted by both Australia and New Zealand.

As part of its analytical efforts, CSIS has identified four categories of IMVE:

- ***Xenophobic violence*** (racially-motivated violence and ethno-nationalist violence): Xenophobic violence can include ideologies such as white supremacy, neo-Nazism and ethno-nationalism. Numerous mass-casualty attackers over the past decade were motivated by xenophobic views. Actions of more recent attackers have been motivated or inspired by previous attackers. In 2017, Alexandre Bissonnette, motivated by ethno-nationalism and rage over Syrian refugees in Canada, shot and killed 6 members of an Islamic Cultural Centre in Quebec City, wounding 19 others. In 2019, Canadian Armed Forces reservist Patrik Mathews, a member of The Base, a neo-Nazi group that is now a listed terrorist entity in Canada, fled to the US where he was later arrested. In October 2021, he was sentenced to nine years in a US prison for plotting serious violence with members of The Base. Most recently, in 2020 Nathaniel Veltman killed 4 members of a Muslim family and injured a child, motivated by xenophobia and inspired by a similar xenophobic attack in Christchurch, New Zealand.

- ***Anti-authority violence*** (anti-government/law enforcement violence, anarchist violence): Anti-authority violence is almost exclusively targeted at governments and law enforcement, and shares accelerationist beliefs with xenophobic narratives. Accelerationism, which is a common belief across many CSIS SOIs (SOIs), is grounded in the idea that Western governments are irreparably corrupt and that multiculturalism and democracy will fail. As a result, there will eventually be an outbreak of violence across ethnic and racial lines – often referred to as "the coming race war". Accelerationists often encourage violence to escalate the pace of societal collapse. The Covid-19 pandemic has led to an increase in anti-authority movements.

- ***Gender-driven violence*** (violent misogyny, including Incel; anti-LGTBQ violence): One growing and concerning area of gender-driven violence is the involuntary celibate (Incel) community. Incels belong to a misogynistic community of males, who associate primarily through online platforms. Though they use a unified terminology, they are not an organized group and have no centralized structure or planning. In Canada, examples of gender-driven violence includes Alek Minassian deliberately running down pedestrians with his van, killing 11 and injuring 15; and an

attack on a spa in Toronto in 2020, perpetrated by a minor who was inspired by the Incel movement, stabbing two women, killing 1 and injuring the other.

- ***Other grievance-driven and ideologically-motivated violence***. IMVE is a fluid environment and threat actors can be driven by a range of grievances that may shift over time. Examples of other grievance-driven IMVE include the Animal Liberation Front, responsible for 20 arsons across the United States resulting in $40 million in damages, anti-abortion driven movements, and direct-action environmentalist groups, such as the Squamish Five who set off a large bomb at the Dunsmuir British Columbia Hydro substation.

The xenophobic and gender-driven violence categories represent the majority of IMVE attacks carried out in Canada to date.

The disruptive effect of global events like the COVID-19 pandemic, the ever-increasing influence of social media and the spread of conspiracy theories has created an uncertain environment ripe for exploitation. Such an environment has the potential to inspire individuals to take violent extremist actions and move their message into the mainstream of society.

The COVID-19 pandemic exacerbated xenophobic and anti-authority narratives. Some violent extremists view COVID-19 as a real but welcome crisis that could hasten the collapse of Western society. Many IMVE threat actors have adopted conspiracy theories about the pandemic in an attempt to rationalize and justify violence.

These narratives have contributed to efforts to undermine trust in the integrity of government and confidence in scientific expertise. While aspects of conspiracy theory rhetoric are a legitimate exercise in free expression, online rhetoric that is increasingly violent and calls for the arrest and execution of specific individuals is of concern.

Over the last few years, CSIS has increased resources dedicated to investigating and analyzing IMVE threats, with approximately fifty percent of Counter Terrorism resources dedicated to IMVE. [7]

2. IMVE intelligence collection pertaining to the Convoy and blockades

2.1. Assessing IMVE in relation to the Convoy

From the beginning of the Convoy and the blockades across the country, CSIS focused on its IMVE SOIs and their activities in relation to those events, while continuing to monitor other streams of intelligence for new or unknown threat actors. CSIS was situationally aware through open source media of several protests throughout 2021 and 2022 focused on public health measures, and in January 2022, began assessing the Convoy in Ottawa in the broader context of rising anti-public health measure movements. These movements were not a homogenous group, but when combined with ever-increasing influence of social media and disruptive elements of the pandemic, created an environment ripe for exploitation by influencers and extremists to commit serious acts of violence.

CSIS assessed that the Convoy provided an opportunity for those with disparate grievances to unify against a perceived common foe. The majority of the participants likely had little to no connection to the

[7] Director of CSIS Appearance on April 26, 2022 at the Special Joint Committee on the Declaration of Emergency

trucking industry, but merely viewed the protest as an opportunity to voice their own personal and ideological grievances. Impacts related to the COVID-19 pandemic have resulted in severe social, economic and psychological effects on individuals and families across a wide spectrum of the Canadian population. Some developed a range of perceived and real grievances that have been motivated by a sense of loss, humiliation, anger and blame, due primarily to underlying factors (e.g. mental health, ideological beliefs and economic situation).

In the lead-up to and during the Convoy protests, CSIS and ITAC communicated regularly with INTERSECT to inform its assessments and to ensure that assessments were available to INTERSECT. INTERSECT is a multi-jurisdictional, all-hazard emergency preparedness program within the National Capital Region for sharing unclassified information within six portfolios (Cyber, Natural Resources, Health, Criminal, Civil Disobedience, Terrorism/Domestic Extremism). INTERSECT did not convene formal meetings during the Convoy.

During the relevant period, CSIS produced five assessments in relation to the Freedom Convoy and the blockades. CSIS cannot provide summaries of these assessments in an unclassified report.

ITAC produced a number of assessments on the protests before, during and after the invocation of the Emergencies Act. These reports were disseminated to government and non-government stakeholders. Along with CSIS' Assistant Director Requirement, the Executive Director of ITAC is a member of ADM-NS Ops[8], which met regularly while the protests, blockades and convoys were occurring. The Executive Director provided updates to the committee on threat assessments as required.

ITAC constantly re-evaluated the threat level during the events. Ultimately, based on available information and intelligence on threats actors' intent and capability to conduct an act of terrorism and given known security mitigation measures in place, the threat level remained at MEDIUM throughout the period of the Convoy protests and blockades.

2.2. Investigations relating to the Convoy

During the Convoy and blockades, CSIS continued to investigate the activities of pre-existing IMVE SOIs in relation to their planned or actual participation in those events, and continued to monitor additional streams of intelligence for any threats previously unknown to the Service, including threat actors that could have used the Convoy as an opportunity to conduct serious violence. This included guarding against potential foreign interference threats. With respect to foreign sources of funding, CSIS' mandate is engaged when funds are provided at the direction of a foreign state with the goal of engaging in foreign interference activities in Canada, or when those donating the money are doing so to support an act of serious violence or terrorism.

During the Convoy, data from the crowdfunding website GiveSendGo was hacked and made public, including the names and citizenship (Canadian and non-Canadian) of the individuals who had donated to the Convoy through that platform. However, because of the legal limitations on CSIS acquiring hacked and leaked datasets described earlier in this report, CSIS did not attempt to access or utilize this dataset

[8] ADMNS-Ops is a committee where Assistant Directors and Assistant Deputy Ministers across a range of federal Government of Canada departments and agencies meet on a recurring basis to discuss issues of operational significance within the national security space.

for its investigations. If CSIS had pursued the path of acquiring and retaining the dataset, it would have required three different approvals amounting to two authorizations: – a ministerial authorization to retain the foreign records and a judicial authorization to retain the Canadian records; This would have been a lengthy process that would have likely concluded after the clearing of the protests in Ottawa, – ultimately diminishing the value of the intelligence that could be derived therefrom. Exigent use of this data, if sought, would have only authorized narrow queries. Other potential forms of collection, such as under section 12 of the *CSIS Act*, require the potential threat to meet the section 2 definition of a threat to the security of Canada. CSIS did not pursue collection of the GiveSendGo dataset under section 12.

2.3. National security threats in relation to the Convoy

Assessing national security threats in relation to the Convoy was challenging due to the fluid and non-homogenous nature of the protests and CSIS' specific mandate. CSIS' mandate and assessment of threats should not be interpreted as definitional of or comprising all national security concerns. CSIS' assessment of threats is based on, and confined by, its mandate and specific role in the broader national security apparatus of the Government of Canada. Therefore, CSIS efforts focused primarily on existing IMVE SOIs and their activities in relation to the Convoy, while continuing to monitor additional streams of intelligence for indications of mobilization to violence, or previously unknown threats.

As stated earlier, the online space is a fertile ground for IMVE actors to interact with each other, attract like-minded individuals and voice their views. In that context, CSIS has observed a rise in violent online rhetoric.

Aspects of conspiracy theory rhetoric online are a legitimate exercise in free expression and can be characterized as "awful but lawful". Violent rhetoric is easily disseminated using both mainstream and alternative media and social media platforms. Many of these platforms leverage encryption technologies to enable threat actors to conceal their identity and evade detection by law enforcement and security agencies, while spreading their message, inciting violence and recruiting like-minded individuals. This same technology, and the nature of the decentralized IMVE space, enables users, to exaggerate or fabricate their capabilities, further challenging the detection of serious threat actors.

It is challenging and resource-intensive for CSIS to determine when and if violent online rhetoric poses a concrete threat of serious violence. Not all extremists are willing to engage in an act of serious violence, but their impact on the threat landscape can still be dangerous and concerning to CSIS. For example, many extremists strive to inspire, encourage or facilitate others to engage in acts of serious violence. Some of CSIS' SOIs use the online space to spur radicalization and spread extremist messaging.

Given this context, in advance of and during the Convoy CSIS maintained awareness of the rhetoric used by IMVE actors, especially against public officials, and the Government of Canada. CSIS observed overt calls by IMVE actors to "hold the line" as well as the public disclosure of directories that included the names of all members of the Ottawa Police Service.

The presence of SOIs and potentially unknown ideological extremists at the protest and the dynamic situation of a mass protest provided an opportunity for IMVE to recruit and potentially radicalize new members.

2.4. Intelligence pertaining to foreign-based IMVE supporters attempting to enter Canada

CSIS leveraged existing relationships with foreign and domestic partners to maintain awareness of any foreign-based IMVE supporters attempting to enter Canada. CSIS cannot provide any further specifics in an unclassified report.

3. Intelligence sharing

3.1. CSIS information sharing protocols with RCMP and other law enforcement agencies

The Service and the RCMP use the *One Vision* framework to govern information sharing as both CSIS and RCMP exercise their separate national security mandates. Since *One Vision*'s launch in 2012, the national security landscape has shifted significantly, necessitating updates to the framework. In 2018, CSIS and the RCMP proactively initiated a review by an independent third party to assist in identifying challenges and solutions to improve cooperation. The Operational Improvement Review resulted in 76 recommendations and ultimately led to the current *One Vision 3.0* framework.

Information sharing from CSIS to the RCMP can take the form of a Use Letter or may occur orally during a meeting. Use Letters state the purpose for which CSIS information can be used, and are clearly caveated to identify to whom and how the RCMP may disseminate the information. When CSIS shares information orally in a meeting, the information is restricted to inform the discussion at the meeting and must not inform any law enforcement investigative action or step unless it is separately provided in a Use Letter. The exception to this is in the case of imminent threat (threat to life or serious bodily harm).

When deciding on the form of information sharing, CSIS takes into consideration (1) the public interest in sharing information; (2) the impact that sharing may have on CSIS' investigations, methodology, and sources; (3) and the impact of any judicial disclosure obligations on CSIS. CSIS and the RCMP, with the assistance of Public Prosecution Service of Canada (PPSC) counsel as appropriate, may discuss their respective understandings of the foregoing matters and mitigation strategies that attempt to address the public interest in sharing, while minimizing potential adverse impacts on CSIS' ability to fulfill its mandate. CSIS has the opportunity to review judicial applications, prior to filing, if a Use Letter will be used by the RCMP to obtain judicial authorization.

The Service also shares information and intelligence with police of jurisdiction. The *One Vision* framework also guides such sharing.

3.2. ITAC information sharing

The 2004 National Security Policy, which is the genesis of ITAC, provided direction for ITAC to disseminate its assessments to "senior government officials, to Canada's intelligence community and ultimately will be used to inform officials as appropriate at the federal, provincial/territorial and municipal levels." Guided by this direction, ITAC is subject to the same legal and policy framework for sharing intelligence as CSIS, including the CSIS-RCMP *One Vision* framework, as well as supporting internal policies and procedures.

Within this legal and policy framework, ITAC actively monitors a range of open and classified sources of information, and has secondees from other departments and agencies who facilitate access to this

information. With respect to law enforcement partners in particular, ITAC is a member of INTERSECT and participates in Combined Intelligence Groups (CIG), which are event-specific temporary measures to bring together intelligence and law enforcement partners in order to centralize information sharing and exchange. A CIG was established for the Freedom Convoy protests. ITAC is solely an assessment body; it does not collect intelligence. As such, ITAC would not disseminate information the way that CSIS or the RCMP might.

3.3. Information shared with the RCMP or other law enforcement agencies

Throughout the Convoy, CSIS and the RCMP worked through the *One Vision* Framework to share relevant intelligence on potential threats to the security of Canada, including information related to CSIS SOIs. CSIS cannot provide specifics relating to the intelligence shared in an unclassified report.

3.4. Cabinet meetings

Advising the Government of Canada about threats to the security of Canada is a fundamental part of the Service's role in protecting Canada and Canadians. In this function, CSIS was invited to attend several Cabinet meetings in early 2022 in relation to the Convoy, including the Safety, Security and Emergencies Cabinet Committee and the Incident Response Group. CSIS' role at those was to provide updates on national security threats that may arise and answer questions.

3.5. Intelligence received from foreign or domestic partners pertaining to the IMVE threats as the Convoy or blockades

CSIS continually monitored streams of intelligence and shared information with domestic and foreign partners, including through the *One Vision* processes with the RCMP and police of jurisdiction to assess threats of serious violence in relation to the Convoy. CSIS cannot provide specific information related to the intelligence received from foreign or domestic partners pertaining to these threats in an unclassified report.