Commissioned Paper:
The Role of Intelligence in Public Order Emergencies

Prepared by: Wesley Wark
Note to Reader

Pursuant to Rules 5-10 of the Commission's Policy Phase Rules of Practice and Procedure, the Commissioner may, in his discretion, engage external experts to produce discussion, research and policy papers, known as "Commissioned Papers".

Any views expressed in a Commissioned Paper are those of the author(s) and do not necessarily reflect the views of the Commissioner. Statements of fact contained in a Commissioned Paper do not necessarily represent the Commissioner’s views. The Commissioner’s findings of fact are based on the evidence presented during the Commission’s hearings.

Parties and members of the public may provide written comments to the Commission in response to this paper. Information about the process for filing comments, including deadlines, are set out in the Commission’s Notice re Policy Phase of the Commission, which is available on the Commission’s website.
“The Role of Intelligence in Public Order Emergencies”

Research paper prepared for the Public Order Emergency Commission
August-September 2022

Dr. Wesley Wark
Senior Fellow
Centre for International Governance Innovation*

(The views expressed in this paper are those of the author and do not necessarily represent those of the Public Order Emergency Commission)
* I wish to thank Morgan Wark, a third year philosophy major at the University of Toronto, for his research assistance in combing through voluminous Parliamentary committee records. The author also wishes to extend his appreciation to two persons who read and commented on an earlier draft. This report benefitted from the willingness of individuals who shared the results of their Access to Information Requests with the author.

Table of Contents

Abbreviations pp. 4-5
Executive Summary pp. 6-7
Introduction pp. 8-9
Organization of the Report p. 9
Understanding intelligence pp. 10-11
On Open-Source Intelligence pp. 11-14
The federal national security intelligence (NSI) community pp. 15-18
Mandates and authorities of relevant NSI entities pp. 18-21
The Emergencies Act pp. 22-23
Intelligence at the Cabinet Table:
The Incident Response Group (IRG) pp. 23-30
The National Security and Intelligence Adviser to the PM pp. 30-31
The role and activities of relevant National Security and Intelligence Entities:
CSIS pp. 32-38
ITAC pp. 39-44
RCMP pp. 44-50
CBSA pp. 50-51
FINTRAC pp. 51-53


On Public intelligence pp. 54-57
On Review and Accountability pp. 57-58
Conclusion: Findings and Issues For Future Study: pp. 58-61
Endnotes pp. 62-72
Abbreviations:

ADM NS OPS: Assistant Deputy Minister Committee on National Security Operations

BCCLA: British Columbia Civil Liberties Association

CBSA: Canada Border Services Agency

CRCC: Civilian Review and Complaints Commission for the RCMP

CSIS: Canadian Security Intelligence Service

EP: Emergency Preparedness Secretariat (PCO)

FINTRAC: Financial Transactions and Reports Analysis Centre of Canada

GOC: Government Operations Centre, Public Safety

IAS: Intelligence Assessment Secretariat, PCO

IMCIT: Ideologically Motivated Criminal Intelligence Team (RCMP)

IMVE: Ideologically Motivated Violent Extremists

INSET: Integrated National Security Enforcement Team (RCMP-led)

IRG: Incident Response Group (Cabinet Committee)

ITAC: Integrated Terrorism Assessment Centre

NSI: National Security and Intelligence

NSIA: National Security and Intelligence Adviser to the Prime Minister

NSICOP: National Security and Intelligence Committee of Parliamentarians

NSIRA: National Security and Intelligence Review Agency
OSINT: Open Source Intelligence

PCO: Privy Council Office

PMO: Prime Minister's Office

RCMP: Royal Canadian Mounted Police

SIRC: Security and Intelligence Review Committee (succeeded by NSIRA in 2019)

SOCMINT: Social Media Intelligence
Executive Summary

Senior Canadian intelligence officials have publicly warned that Canada is facing a pivotal moment in dealing with a changing and volatile national security threat environment. In June 2021, the National Security and Intelligence Adviser to the Prime Minister stated:

“The world is at an inflection point...facing a complex combination of new and enduring national security challenges...National security threats against Canada — whether from state or non-state actors or global phenomena such as pandemics and climate change— are greater than ever and directly impact our economy, our democratic institutions, and our way of life. In the face of such massive change, Canada’s national security and intelligence community needs to evolve and adapt.”

Two recent examples of national security challenges came hard on the heels of each other in early 2022—the protests conducted under the umbrella of the so-called “Freedom Convoy,” and the premeditated and brutal Russian invasion of Ukraine.

Canada’s national security and intelligence system plays a fundamental role in allowing the federal government to understand the threats the country faces and respond accordingly. That role involves providing intelligence on the intentions, capabilities and operations of threat actors. Intelligence encompasses early warning and situational awareness. All of these functions were vital to intelligence performance with respect to the “Freedom Convoy” protests.

Two related issues must be faced squarely: whether Canada suffered an intelligence failure in monitoring the “Freedom Convoy;” and whether that intelligence failure affected the decision of the government to invoke the Emergencies Act on February 14, 2022. Intelligence failure can be a loaded issue and sometimes a matter for scapegoating. What deserves serious attention is the accuracy and relevance of the available intelligence on the “Freedom Convoy,” and whether it informed policy making appropriately. In this research paper there are indications of intelligence success and worrying signs of failure, including with regards to the governance of the national security and intelligence system. Full answers can only be known through more systematic study and access to classified records.

This research paper begins with a general analysis of intelligence as a function of government and proceeds to examine the activities of key national security and intelligence organizations, from the Cabinet table to entities with very specialised mandates.
The conclusion to the paper offers some findings and suggestions for necessary changes to legislation and governance, based on the analysis contained herein. Key questions to be addressed in the text include:

*Were there perceived authority limitations that impeded the ability of national security and intelligence entities to collect, process, analyse and disseminate intelligence on the “Freedom Convoy”?*

*Were intelligence collection methods, especially open source, properly utilised?*

*Was intelligence reporting from a variety of departments and agencies fully integrated?*

*Were intelligence assessments on the national security threat posed by the “Freedom Convoy” accurate, relevant, and sufficiently forward-looking?*

*Was the dissemination of intelligence to decision-makers timely and effective?*

If the answer to any of these questions is no, then there is urgent work to be done to improve the authorities, capabilities and reporting mechanisms of the national security and intelligence system. At the same time, it is important to ensure that political decision makers fully understand and trust the intelligence they receive.

In any future circumstance where a federal government might need to reach for extraordinary powers, as with the Emergencies Act, it is important to avoid a circumstance where inadequate intelligence, or lack of confidence in intelligence, or an inadequate national security and intelligence governance system, compels the use of such powers.

The research paper ends with a quote from the CSIS Director, David Vigneault, in which all Canadians should be invested:

“the fight for democracy is one we cannot afford to lose.”

The national security and intelligence system must be equipped for that fight, in ways that the Canadian public will understand and accept. The available evidence and tentative judgement in this paper is that the NSI system was not ready and fully equipped when the “Freedom Convoy” descended on Ottawa and critical infrastructure at the border.
**Introduction:**

It has repeatedly been said, and demonstrated in recent public opinion polling, that Canadians know little about their country’s national security system. A lack of understanding about national security may seriously hamper public discourse and weaken the fabric of our democratic processes. It is abetted by the secrecy that continues to surround national security practices in Canada. Lack of public knowledge and secrecy can give oxygen to conspiracy theories, as was demonstrated during the “Freedom Convoy.”

Understanding national security is also complicated by the inevitable tensions that arise in a democracy between practices aimed at achieving security and those designed to ensure the maintenance of our rights and civil liberties. National security discourse often carries with it the ball and chain of societal fears of “Big Brother.” Extremist anti-government rhetoric only deepens such fears. Academic discussion can be hampered by ill-defined concerns about “securitization.”

The role that national security and intelligence organizations play in defending the state and society against threats has been torqued by new challenges. These include foreign interference, the malicious spread of disinformation, rampant espionage, cyber threats, and the undermining of Canadian economic security. Democracy itself is being challenged by a new threat environment in which authoritarian movements are on the rise globally and anti-government conspiracy theories flourish across the internet. Transnational threats to security posed by pandemics and climate change impacts are imposing increasingly stiff costs domestically and internationally.

In February 2022, for a brief period of nine days, the government of Canada took the unprecedented step of invoking the Emergencies Act and declaring a Public Order Emergency, in response to a protest movement that called itself the “Freedom Convoy” and had encamped in the nation’s capital and blockaded key border crossings between Canada and the U.S.

Investigating the role that intelligence played in advising the government on the threat posed by the “Freedom Convoy” is essential to any understanding of the rationale for the government’s decision to invoke the Emergencies Act. This role is not singular and frozen in time. What happened in the lead up to February 14, 2022, must also be understood as an object lesson in how intelligence should perform in the future when protest movements, or other dangers, may again be seen to threaten national security.

Two questions must be at the heart of any examination of the role of intelligence in responding to protest movements that raise legitimate national security concerns. One is whether the intelligence system was able to deliver useful warning and situational intelligence to assist the
government in decision-making about how to respond to the protest. The other is whether the governance arrangements for the intelligence system were shown to be in working order and effective. These are large issues that can never be addressed properly without access to the full classified record. But an initial examination based on publicly available records can be a starting point by identifying problem areas and raising questions for further study.

This study is based entirely on publicly available records extant between July and early September 2022, when the research and writing was conducted. It has been aided by the partial release of Cabinet records, by testimony given by government officials to Parliament, by publicly available court records, and by material released in response to Access to Information requests.\(^8\) But none of this amounts to anything like a full record. This study takes no position on the legitimacy or otherwise of the government’s decision to invoke the Emergencies Act and it does not seek to pronounce on whatever national security threats the protest movement may have presented.\(^9\) It is designed to elucidate how the Canadian national security intelligence system responded to the “Freedom Convoy” protests.

The observations and analysis in this report are based on my own study of the available record and on my own knowledge of Canada’s national security and intelligence system. The views expressed in this report are my own personal opinion. I hope they may be of use.

**Organization of the Report**

The report focuses entirely on the federal government’s national security and intelligence (NSI) system. The federal government has unique carriage of national security threats and deploys intelligence resources unavailable to other levels of government. The report does not include any study of security, intelligence and law enforcement practices at the provincial, territorial or municipal levels.

The study throughout refers to the “Freedom Convoy” as an object of the work of the federal national security and intelligence system.

The study examines events during January and February 2022, but does not consider the impacts of the invocation of the Emergencies Act on the work of the NSI community.

The study is broken down into component discussions, some general and high level regarding the nature of intelligence, the organization of the federal national security and intelligence community, the mandates and authorities of relevant NSI departments and agencies and the intersection between the Emergencies Act and the CSIS Act. It also looks at the known role played by various actors in the national security and intelligence space, from the Cabinet and National Security and Intelligence Adviser, through to specific entities with intelligence roles. It raises a speculative question about public intelligence and briefly discusses the importance of review and accountability.
Each component discussion is indicated by sub-headings in the report for ease of reference. Readers can refer to the Table of Contents for guidance to specific sections.

**Understanding Intelligence**

In the 2004 National Security Policy, the only extant national security strategy issued by the Canadian government, intelligence is described as “the foundation of our ability to take effective measures to provide for the security of Canada and Canadians. To manage risk effectively we need the best possible information about the threats we face and about the intentions, capabilities and activities of those who would do us harm.”

This statement, while generic, does identify some of the principal features of intelligence—that it deals with threats to security; that the quality of intelligence matters; and that the focus of intelligence is on the intentions, capabilities and operations of threat actors.

In addition to these general features, it is important to understand that intelligence is a complex enterprise, often portrayed in the form of an intelligence “cycle” representing different elements of the genesis of intelligence knowledge with collection, analysis and dissemination at the core. An intelligence picture will always be incomplete to some degree. This puts extra emphasis on maximising collection, building in corroboration of information, ensuring analysis/assessment is of the highest quality, providing for the timely dissemination of intelligence, and ensuring that decision-makers understand the strengths and weaknesses of an intelligence product. Building and maintaining a system that operates to these goals is often referred to as facilitating a strong intelligence “culture.”

While the subject matter of intelligence may be described as understanding threats to security, its objective goes beyond understanding, to encompass a notion of ‘competitive’ or ‘informational advantage.’ That is, entities look to intelligence to provide warning, which may be elastic and future-oriented, and current situational awareness. If warning and situational awareness are sufficiently accurate, this helps to identify opportunities for action and generate optimal decision-making.

One more distinction to add to the mix concerns what is often called “actionable” intelligence, which is particularly important in dealing with unfamiliar or novel situations of surprise. Actionable intelligence needs to be timely, relevant to decision-makers, and of a precision that enables decision-makers to use it in responding to an emerging threat. This is the formula advanced by Erik Dahl in his major study of intelligence and surprise attack. As Dahl also notes, actionable intelligence must be met with receptivity and understanding of the intelligence process on the part of decision-makers.

The 2004 National Security Policy made clear the link between intelligence and security. Intelligence is a means by which security can be achieved. National security is situated as the
highest obligation and greatest goal of government, even if this concept is rarely addressed in Canadian public discourse.  

But as a means to an important end, intelligence is also fraught with controversy. The very nature of intelligence, its attendant secrecy, its mystique, driven by popular culture depictions, its potential intrusiveness, all combine to generate natural concerns in democratic societies. A former senior UK intelligence official, Sir David Omand, has identified a significant contemporary shift in thinking about the security-intelligence linkage by arguing that:

"national security today should be defined as a state of trust on the part of the citizen that the risks to everyday life, whether from man-made threats or impersonal hazards, are being adequately managed to the extent there is confidence that normal life can continue."  

Maintaining citizen trust and “carrying on” is a challenging goal in an age of political polarization, declining democratic norms, rampant misinformation and disinformation, and loss of faith in authority structures. Quite apart from these meta trends the idea of citizen trust more specifically in intelligence and the pursuit of security butts up against engrained ideas of intelligence as posing dangers to democracy and rights, especially as new technologies of information gathering and analysis provide new tools for intelligence agencies. The 2004 National Security Policy, penned in a different technological and threat era from today, tried to put a brave face on the existential dilemma of security policy by arguing that “there is no conflict between a commitment to security and a commitment to or most deeply held values." Better to recognize that tensions may often arise, or be perceived to arise, between the pursuit of security and the maintenance of democratic rights. How those tensions are managed through legislation, policy, action, accountability and public transparency are key.

The invocation of the Emergencies Act by the government on February 14, 2022, raises profound questions about the uses of intelligence, the pursuit of security, and the ongoing maintenance of citizen trust in a democracy. Paradoxically, growing reliance by security and law enforcement agencies on open-source intelligence in responding to potential threats to national security can be at the heart of this dilemma.

**On Open-Source intelligence (OSINT)**

Open-Source intelligence is one of many intelligence collection methodologies (often referred to as “ints”). While it is of long-standing, it has been transformed by the volume and speed of information transiting the internet, information circulating on social media platforms, and information captured in data bases.

Sir Mark Rowley, the newly appointed head of the UK Metropolitan Police, and former head of UK counter-terrorism policing, has recently written that:
“OSINT can be a powerful intelligence and investigative tool but it is too often overlooked. In many organizations there are significant barriers to the adoption of effective OSINT, as well as a failure to adapt fast enough to emerging technologies. A cultural shift is needed in order to elevate the status of OSINT and ensure that it is used to its full potential.”

The barriers that Sir Mark referenced include misunderstandings about OSINT, which despite its many recent successes in the hands of NGOs such as Bellingcat, can “conjure a somewhat negative image, with connotations of hacker-like behaviour and invasions of privacy.”

Definitions of OSINT can go some way to addressing these misconceptions. The US intelligence community has an official definition of OSINT:

“produced from publicly available information that is collected, exploited and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement”

The literature on OSINT offers many definitional variants. Stevyn Gibson offers this one: OSINT is, “the exploitation of information legally available in the public domain.” But as Gibson also notes the definition is problematic in all its parts—including the notion of what constitutes the public domain, the concept of ‘legally available’ and the matter of who does the exploitation, particularly when government intelligence services have no monopoly over OSINT and may benefit from working in partnership with private sector firms and NGOs.

Sir David Omand and his co-authors take a different approach to what they describe as “social media intelligence” (or SOCMINT) and argue that its potential must be anchored in concepts of necessity and legitimacy. Necessity involves an ability to demonstrate its applied use to advance public safety goals. Legitimacy, in their view, can be framed by principles drawn from just war doctrine, include right cause, motive, authority and proportionate use. They remind readers, flipping the just war doctrine on its head, that secret intelligence should be a last recourse because of its intrusive potential; social media intelligence should be a first recourse.

If precisely framing OSINT (or SOCMINT) is difficult, its attributes are easier to determine. These attributes include: accessibility and relative low cost compared to more clandestine methods of intelligence collection; the flexibility it offers, particularly in terms of a surge capacity when more information on a particular target is urgently needed and other intelligence collection methodologies cannot be pivoted as quickly; and the ability of OSINT to serve as a gateway to more precise targeting. Finally, there is the practical benefit for security and intelligence systems of the lower classification levels for reporting derived from OSINT, which makes reporting products easier to circulate and gives them potentially much wider readership.

OSINT has one characteristic that is both benefit and drawback: the volume of information available. To make use of OSINT’s richness requires sophisticated technological tools, such as artificial intelligence and machine learning, and human analytical capacity.
But for all these attributes there is, counter-intuitively, an ongoing challenge with the deployment of OSINT. This involves the question of lawful authorities. Where more clandestine and intrusive methods of intelligence collection can be protected through a judicial authorization system, along with other accountability checks, the same is less true for OSINT. Warranted OSINT would be, in most cases, a contradiction in terms, but this leaves open the boundaries around lawful collection, which is further complicated by the fast pace of technological change and pressures on traditional definitions of privacy. As a Library of Parliament report by Holly Porteous puts it, “pervasive digitalization raises difficult legal and ethical questions about what can reasonably expected to remain private and the extent to which an individual can control what happens to their personal information while continuing to participate in society.” In the Canadian context, these pressures are also framed by Charter protections against unreasonable search and seizure. Both the RCMP and CSIS have found themselves caught up in this dilemma, as my report demonstrates below.

The content of social media messaging could (and should) have provided national security and intelligence agencies with their best source of important clues about the intentions, capabilities and operations of the “Freedom Convoy” protest. Utilization of this source would have required an early determination about potential threats to national security posed by the protest, a sophisticated technological capacity to collect and assess the flow of information across mobile devices and the internet, both domestically and internationally, and timely action as discourse about the Freedom Convoy metastasized online. It would have required an appropriate governance framework to ensure effective use of OSINT, particularly in terms of analysis and dissemination.

Even in the absence of a full-scale examination of the social media activity of the “Freedom Convoy,” the value of the material for national security and intelligence purposes seems clear. One indicator is a 4,000 page document detailing communications between two of the convoy organizers, Tamara Lich and Chris Barber, that was entered as evidence by the Crown in a bail hearing for Lich.

The Verge, a multimedia organization founded in 2011, that tracks the intersection of technology and culture, curated one investigation into the “Freedom Convoy’s” Facebook ecosystem. It identified an informational “pipeline” that moved from physical protest to social media to right wing establishment outlets. It was that pipeline that gave the “Freedom Convoy” its global presence. The Verge tracked the rise of the “Freedom Convoy” on Facebook tracing its initial start to a post on Rumble, a right-wing video platform, on January 18, 2022, which was then picked up by a Facebook page called “Freedom Convoy 2022” which linked to another far-right activist, Pat King. Mentions for “convoy” across the web jumped enormously between January 25 and January 29, the beginning of the weekend demonstrations in Ottawa. As The Verge investigation found, the centre of gravity of the “Freedom Convoy” on Facebook had moved offshore by the end of January, with the largest Facebook group—“The People’s Convoy-official” run by five administrators with U.S. ties. The analysis concludes that the social media presence of the “Freedom Convoy” initially involved a “small collection of local
conspiracy theorists”, but it was “given a megaphone by America’s powerful right-wing disinformation machine.” 27

Foreign content mills also emerged as the amplification of the “Freedom Convoy” message took off online. One was run from Bangladesh. 28 Another from Bulgaria. 29 One investigation found that some of the largest Facebook groups involved in promoting the “Freedom Convoy” in the run-up to the arrival of demonstrators in Ottawa over the weekend of January 29-30, were being run through a stolen account belonging to a Missouri woman. Facebook moved to disable the illicit accounts on February 7. 30 The Canadian Anti-Hate coalition, early in the “Freedom Convoy’s” evolution, identified the significance of the “Freedom Convoy’s” crowd funding efforts and the role that far-right organizers, such as Pat King, and the accelerationist movement, Diagolon, played. 31

The tracking and analysis by small media organizations and NGOs shows the potential of open-source intelligence when it comes to understanding the inner world of a protest movement and the ways in which its messaging can reach far beyond a small coterie to have global impacts, including reputational impacts for Canada.

Measuring the degree of success or failure involved in the national security and intelligence community’s efforts to deploy OSINT capabilities to understand the potential threats to national security presented by the “Freedom Convoy” is critical. There are two observations in play. One is that, in recent months, the combination of the “Freedom Convoy” protests at home and the momentous implications of the Russian invasion of Ukraine, where open-source intelligence has played such a prominent role, remind us of the vital importance of treating OSINT as a prime intelligence resource and, as Sir David Omand suggests, a first recourse of the national security intelligence system when faced with an emerging threat.

The second is that with heightened appreciation of the importance of OSINT as an intelligence tool, governance needs to be altered to match. Two recent Canadian reports have both called for enhancements to the national security and intelligence community’s capacities for OSINT. Greg Fyffe has argued that there should be a common OSINT platform for the Canadian intelligence community, coordinated by a senior official. 32 A separate report by the “Task Force on National Security,” asked “who in the government should be responsible for monitoring social media?” noting that partial mandates existed in numerous organizations. In the case of the “Freedom Convoy,” the Task Force authors believe that government mandates to collect social media intelligence were “strictly limited.” Like the Fyffe report, the Task Force proposed the option of creating a stand-alone unit to collect and analyze open-source. The idea of having it placed in Public Safety alongside a small unit that engages in community counter-radicalization funding may be less attractive than placing the unit directly in the Privy Council Office, alongside the Intelligence Assessment Secretariat, and reporting to the National Security and Intelligence Adviser. 33

Machinery of government changes always warrant careful reflection. But change to ensure a
much enhanced capacity for OSINT collection, analysis and use is vital for both law enforcement and intelligence agencies.

**The Canadian National Security and Intelligence (NSI) system**

The structure and operations of the federal government’s intelligence community are opaque to most Canadians. Recent public opinion surveys conducted by both CSIS and CSE indicate low levels of public knowledge about these organizations, a finding bound to be replicated in any understanding of the broader intelligence system. 34

The Privy Council Office published a small pamphlet in 2001 describing the Canadian security and intelligence community, complete with an organization chart. 35 It described the S and I community as a “significant national asset.” The pamphlet’s discussion of intelligence was kept at the most elementary level, but notably included a mention of open-source intelligence as a counter-point to secret intelligence:

“some components within the community possess a unique capability and authority to collect and assess information that is not available from conventional sources—in other words secret information. In doing their work, security and intelligence community staff must blend this information with all other available information, including openly-available information from international broadcasts, newspapers, the Internet and academia, other parts of government, and intelligence generated by foreign countries.” 36

There has been no official public update of this basic accounting of the intelligence community since 2001.

However, the first annual report of the National Security and Intelligence Committee of Parliamentarians, submitted to the Prime Minister in December 2018 and published in April 2019, included a chapter on “A Functional Overview of the Security and Intelligence Community.” The chapter wrestled with definitions of national security and intelligence, noting that neither is defined in legislation, the closest being the enumeration of threats to the security of Canada set out in the CSIS Act. The NSICOP report also addressed the question of the organization of the security and intelligence community, drawing on, but adapting, material supplied to it by the Privy Council Office.

The organization chart that the committee came up with distinguishes between eight “core” federal organizations, with mandates that are “entirely or substantially related to national security, intelligence or both,” and an outer ring of organizations that belong to the security and intelligence community but have mandates broader than security and intelligence.

The eight core members are listed as: 37

*The National Security and Intelligence Adviser*
Canadian Security Intelligence Service

Department of National Defence/Canadian Armed Forces

Canada Border Services Agency

Communications Security Establishment

Royal Canadian Mounted Police

Global Affairs Canada

Integrated Terrorism Assessment Centre
Of the eight core members, two organizations—CSIS and the RCMP—have important roles in intelligence collection regarding national security threats generated from within Canada. A third, the Integrated Terrorism Assessment Centre, has an analytic role in addressing terrorism-related threats. The Canada Border Services Agency has a niche role as an intelligence collector but is an important consumer and user of intelligence to fulfill its mandate to ensure border integrity at ports of entry and to reach decisions on admissibility of persons and goods to Canada.

Three of the core members have intelligence mandates that primarily concern the global threat environment—Department of National Defence/CAF; The Communications Security Establishment; Global Affairs Canada. These will not be treated in my report.
Several entities not listed by NSICOP as core members of the security and intelligence community—FINTRAC, the Government Operations Centre, and the Emergency Preparedness Secretariat at PCO—are examined in my report because of their relevance or potential in responding to the “Freedom Convoy” protests.

The governance of the national security and intelligence community begins with the Prime Minister and Cabinet. There is currently no dedicated Cabinet committee for national security and intelligence. There are committees on “Canada and the World,” which could consider national security-related issues; and on “Safety, Security and Emergencies,” chaired by the Minister for Emergency Preparedness. The mandate of the Safety, Security and Emergencies committee is described as follows:

“Considers threats and risks to the safety and security of Canada and Canadians, manages ongoing emergencies, and ensures strategic, integrated and forward-looking leadership for emergency management.”

There is also the Incident Response Group (IRG), described as a “dedicated emergency committee in the event of a national crisis or during incidents elsewhere that have major implications for Canada.” Membership of the IRG is determined on a case-by-case basis.

The Incident Response Group was called together for the first time on February 10, 2022, to consider the “Freedom Convoy” protest activities. It would appear to have been the most significant Cabinet committee engaged on the protest, and was chaired by the Prime Minister. A separate section of this report details what is known from redacted records about its discussions prior to the invocation of the Emergencies Act.

Below the level of the Prime Minister and Cabinet there is a cascading system of committees at the Deputy Minister, Assistant Deputy Minister and Director General levels that bring relevant officials from across the community together for policy and operational discussions on national security and intelligence issues. At the head of this committee system, operating from the Privy Council Office and reporting to the Clerk of the Privy Council, is the Prime Minister’s National Security and Intelligence Adviser. The office of the NSIA is a lynch pin in trying to ensure that a decentralised system with individual departments and agencies responsible to Ministers, can be coordinated and made to work together. The NSIA is also a key point of connectivity between the national security and intelligence community and the Prime Minister and Cabinet. The NSIA played a lead role in briefing the Cabinet Incident Response Group on developments with regard to the Freedom Convoy protest and in bringing deputy ministers together in the Deputy Ministers Operations Committee, which she chairs. Two entities within the PCO structure serve the NSIA—the Security and Intelligence Secretariat for operational issues (colloquially known as the “hair on fire” gang) and the Intelligence Assessment Secretariat for strategic threat assessments. Because of the important role played by the NSIA in the crisis a separate section of the report is devoted to that office and its functions.
The governance architecture of the Canadian national security system has changed over time, as new entities have been added and new authorities created. But a consistent feature since the earliest days of a post-1945 Canadian intelligence system has been its decentralised nature, the diffusion of responsibility across many different departments and agencies, and reliance on a sub-Cabinet committee system, with relatively weak central controls. Another persistent feature has been the relative disengagement by Cabinet and successive Prime Ministers from national security and intelligence issues, an aspect of Cabinet governance that began to change significantly after 9/11. But the current absence of a dedicated Cabinet committee on national security and intelligence is one sign of an ongoing failure to ensure that national security and intelligence issues are truly at the heart of federal government decision-making.

As some recent independent reports have emphasised, Canada is an outlier among its Five Eyes and G7 partners in not having a permanent body at the cabinet level chaired by the Prime Minister with responsibility for national security. Two of our leading Five Eyes partners have either long-established (US) or newly established (UK) National Security Council structures. Australia has a strong national security division in the Prime Minister’s office. They offer lessons from which Canada can draw best practices.

The national security and intelligence governance system was challenged by the unprecedented nature of the “Freedom Convoy” protest movement. Reflecting on this experience should be a trigger for a thorough-going examination of the governance mechanisms, capacities and authorities of the security and intelligence community. Organizational change is never sufficient to guarantee success in the face of national security challenges, but without a properly functioning NSI system, human talent and effort can go to waste.

**Mandates and Authorities of Relevant NSI entities:**

The relevant “core” members of Canada’s national security and intelligence community examined in this report operate under a diffuse set of statutory and other authorities. Some have no direct statutory authority for their intelligence gathering and national security activities—this would include the National Security and Intelligence Adviser and the elements of PCO that report to her, CBSA, the Government Operations Centre and the Emergency Preparedness Secretariat. ITAC operates under the strictures of the CSIS Act but is not directly mentioned in it. The RCMP Act contains little direct mention of national security, but RCMP activities in the national security space are undertaken in accordance with the Security Offences Act. The Security Offences Act links an RCMP role in national security investigations to the CSIS Act definition of the threats to the security of Canada, and was created at the same time.

To add to the complexity of the legislative picture, there are currently no legal definitions of national security, intelligence, or open-source intelligence in statute.
No one Minister is responsible for all elements of the national security and intelligence system. But ministerial accountability for four key core elements of the system—CSIS, ITAC, the RCMP, and CBSA—as well as the Government Operations Centre, is exercised by the Minister for Public Safety. A recent reorganization of Cabinet bifurcated the Public Safety portfolio to create a separate Minister for Emergency Preparedness, with a secretariat based at the Privy Council Office to assist him.

All entities in the national security and intelligence community are subject to the government’s intelligence priorities and the disseminated process of “Standing Intelligence Requirements.” But among the constituent members of the security and intelligence community, only CSE is bound by statute to conduct its foreign intelligence gathering activities according to the government’s intelligence priorities. A review of the national security and intelligence system could examine whether meeting government intelligence priorities should be a more widespread statutory obligation.

Intelligence sharing among the elements of the Canadian national security and intelligence community is managed through memoranda of understanding and through the provisions of the Security of Canada Information Disclosure Act (2019), a modification of earlier legislation passed in 2015 (known as SCISA—Security of Canada Information Sharing Act). The essence of the SCIDA regime, which involves some complexity in operationalization, is that for agencies to share intelligence with a government counterpart they must be sure that the receiving organization has the appropriate mandate to acquire such information, and agencies receiving intelligence must determine that it is appropriate to their mandate. The National Security and Intelligence Review Agency is charged with undertaking compliance reviews of SCIDA annually.

All elements of the Canadian national security and intelligence community are now subject to external review from the National Security and Intelligence Review Agency (created in 2019) and the National Security and Intelligence Committee of Parliamentarians (created in 2017). But because of the relativeness newness of the revamped review system, not all constituents of the intelligence community have yet been touched by external review reporting.

The closest there is to one statutory “ring” that binds the practices of the national security and intelligence community is to be found in the CSIS Act that established the new Canadian Security Intelligence Service upon its creation in 1984. This is especially true regarding the definition of threats to the security of Canada found at section 2 of the Act. While some parts of the CSIS Act have been updated since 1984 and new powers added, s2 of the Act remains unchanged and of Cold War vintage.

Not only is that definition of threats to the security of Canada integral to CSIS activities and those of other entities in the national security system, it is also imported into the Emergencies Act as a key threshold.
Section 2 of the CSIS Act lists four elements that comprise the legal definition of threats to the security of Canada. They are (to paraphrase):

a) Espionage or sabotage

b) Clandestine or deceptive foreign influenced activities

c) Threats or use of serious violence

d) Undermining or attempting to overthrow constitutional government

Of these four elements, espionage investigations are a constant preoccupation of the Service, as have been counter-terrorism investigations, captured by part c). Foreign interference, covered by part b) is a growing preoccupation. The subversion focus of part d) is a holdover and CSIS has hardly ever been engaged on such investigations since it took over responsibility for national security intelligence from the RCMP.

Of these four elements, the only one not potentially engaged by the activities of the Freedom Convoy protests was a) espionage. Because it was ultimately relied on by the Governor in Council in invoking the Emergencies Act, the wording of c) is of particular importance. It reads in whole:

“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”

Parts of this definition were imported into the criminal code with the passage of Canada’s first anti-terrorism act in 2001. Terrorism is similarly defined as involving acts or threats of violence for political, religious or ideological motives and there is an element of the criminal code definition of terrorism which refers to “serious interference with or serious disruption of an essential service, facility or system.” While the criminal code definition of terrorism has distinctive features as well, what generally aligns the CSIS Act and the terrorism definition are references that protect “advocacy, protest or dissent.” However, the criminal code definition of terrorism did not import the concept of “lawful advocacy” from the CSIS Act, a matter that incurred much debate during passage of the Anti-terrorism act in 2001. The CSIS Act boundaries around lawful advocacy, protest and dissent, present an important and challenging factor in determining the authority of national security agencies to collect intelligence on protest movements. It is a democratically-spirited inhibitor against intelligence collection, requiring judgement about when a protest movement may move from lawful to unlawful behaviour.

There are other elements of the CSIS Act that bear on the circumstances of the Freedom Convoy protest and delimit CSIS’s sphere of operations. An important one, that also dates back to the original CSIS Act is section 12(1), which provides CSIS’s authority for intelligence collection. S12(1) contains a “strictly necessary” provision:
“The Service shall collect, by investigation or otherwise, to the extent that is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threat to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.”

It should also be noted that CSIS has newer statutory powers for threat reduction measures, first passed in 2015, and for data mining activities, codified in 2019. The data mining regime (section 11 of the CSIS Act) is complex and won’t be analysed here, except to say that the Service may “retain, query and exploit” a publicly available dataset (s11.11(1)). Publicly available datasets are distinguished in the act from “Canadian” and from “foreign” datasets. There are higher fences around retaining, querying and exploiting Canadian datasets, which do not apply to “publicly available” datasets.

Threat reductions measures, first passed into law in 2015, and modified in statute in 2019 may be taken by the Service, “if there are reasonable ground to believe that a particular activity constitutes a threat to the security of Canada” (s12.1(1)). Threat reduction measures are meant to be preventive, but it is not known if CSIS had recourse to these powers or to the use of its data mining regime in response to the “Freedom Convoy” protests.

The centrality of the CSIS Act definition of threats to the security of Canada extends to the financial intelligence unit known as FINTRAC, the Financial Transactions and Reports Analysis Centre of Canada. FINTRAC legislation is included as Part 3 of the “Proceeds of Crime (Money Laundering) and Terrorist Financing Act,” first passed in 2000 and subsequently amended in December 2001 to include intelligence sharing on suspected terrorist financing.

Provisions of the CSIS Act have become embedded more broadly in national security law in Canada, especially regarding threats to the security of Canada. Given their closeness in time, and the ways in which the CSIS Act emerged out of the recommendations of a major judicial inquiry and lengthy deliberations by Parliament, it is little surprise that the CSIS Act definition of security threats was made to constitute one threshold for invocation when the Emergencies Act was passed four years later, in 1988.

**Emergencies Act**

The Emergencies Act contemplates four different kinds of emergencies: a public welfare emergency; a public order emergency; an international emergency; and a war emergency.

The Governor in Council invoked Part 2 of the Act, a public order emergency, on February 14, 2022. Declaration of a public order emergency requires that two thresholds be met, captured in the definition: “a public order emergency means an emergency that arises from threats to
the security of Canada and that is so serious as to be a national emergency.” National emergency is defined at section 3 of the Act and, in turn, comprises two components.

“a national emergency is an urgent and critical situation of a temporary nature that

   a) seriously endangers the lives, health or safety of Canadians and is of such proportions or nature as to exceed the capacity or authority of a province to deal with it, or
   b) seriously threatens the ability of the Government to preserve the sovereignty, security and territorial integrity of Canada

and that cannot be effectively dealt with under any other law of Canada.”

The two-part construction of a national emergency, in short, involves, firstly, a determination of its seriousness and of the absence of an effective alternative in other recourse under the law.

The second threshold for a Public Order emergency is that it must meet the meaning assigned to threats to the security of Canada in section 2 of the CSIS Act, discussed above. At least one of the four definitions of security threat must be found to apply.

The proclamation of the Public Order Emergency by the Governor in Council on February 15 declared that a public order emergency existed because of five conditions: 58

Continuing blockades

Threats to economic security resulting from the impacts of blockades of critical infrastructure

Adverse effects on Canada’s relationship with its trading partners

Breakdowns in supply chains and the risk these breakdowns will continue

The potential “for an increase in the level of unrest and violence that would further threaten the safety and security of Canada.”

There is no direct reference in the language of the 1988 Emergencies Act to threats to critical infrastructure, Canada’s international relations, or supply chains. Where the CSIS Act definition of threat to the security of Canada is called into play by the proclamation is in reference to the first and fifth conditions set out in the proclamation, and most explicitly with regard to the first condition, reproduced in full here:

“the continuing blockades by both persons and motor vehicles that is occurring at various locations throughout Canada and the continuing threats to oppose measures to remove the blockades, including by force, which blockades are being carried out in conjunction with activities that are directed towards or in support of the threat or use of acts of serious
violence against persons or property, including critical infrastructure, for the purpose of achieving a political or ideological objective within Canada.”

In other words, the invocation of a Public Order Emergency relied on part c) of s2 of the CSIS Act to meet the threshold of a threat to the security of Canada.

The significance of this is that the Governor in Council determined that a threat to the security of Canada as defined in the CSIS Act existed by February 14 and was sufficient, in part, to declare a Public Order Emergency. It is important to move back in time from this moment to try to understand how national security and intelligence agencies may have responded, on reasonable grounds (as per the CSIS Act), to perceived threats to national security posed by the “Freedom Convoy.” In order to engage national security and intelligence agencies, such threats must go beyond lawful protest, advocacy and dissent.

The next sections of this report look at how different entities in the federal government NSI community may have operationalized mandate authorities to collect and analyse intelligence on the threat and advise government.

**Intelligence at the Cabinet Table: The Incident Response Group**

The Incident Response Group (IRG) is an ad-hoc Cabinet committee established in 2018, comprised of selected Cabinet ministers and their officials, who meet on an as-needed basis to deal with a national crisis or a major international event. It appears modelled on a long-standing British Cabinet committee that deals with national emergencies known as COBR/COBRA.

The Incident Response Group played a key role in Cabinet-level decision making in the lead up to the invocation of the Emergencies Act on February 14. It also held meetings during the period when the Emergencies Act was in force, before turning its full attention to the situation of the war in Ukraine. Aside from some statements released by PMO summarising the meetings of the IRG, there is a partial, redacted record of the minutes of IRG meetings made available to litigants before the Federal court seeking to challenge the lawfulness of the invocation of the Emergencies Act. These records, even in their redacted form, provide some important insights into the issues that the IRG was dealing with.

The IRG was convened on three occasions prior to the invocation of the Emergencies Act. In every case the Prime Minister chaired the meeting.

The first meeting took place on Thursday, February 10, fully two weeks after the first convoy of trucks had entered Ottawa and emplaced themselves in the downtown core and parliamentary precinct. Four days previously the city of Ottawa had declared a state of emergency. A third border blockade had begun in Emerson, Manitoba, alongside the earlier and on-going blockades at Coutts, Alberta and at the Ambassador bridge in Windsor, Ontario. On February
10, the federal Conservative party began to shift its previous position in support of the “Freedom Convoy” protesters by calling for an end to border blockades. The Prime Minister was scheduled to hold a call with the US President to discuss ending the border blockades on the following day.

The National Security and Intelligence adviser was the lead briefer to the IRG at the first two meetings on February 10 and 12. On February 10, she noted that an “integrated planning cell” was developing a plan of action. She stated that the preference remains to seek a negotiated solution to the protests but that enforcement actions could start the following week if negotiations were unsuccessful. In discussing specific actions that could be taken, the redacted IRG minutes note that the Prime Minister discussed two possible tracks: actions that could be taken under existing authorities; and the invocation of the Emergencies Act.62

A second meeting of the IRG was held two days later, on Saturday, February 12. On this day the media reported that an estimated 4,000 protesters had converged on Parliament Hill. A large sound stage had been set up by the protesters as well as a hot tub. Counter-protest activity was beginning to take shape in Ottawa, accompanied by demands that the Ottawa Police Service (OPS) take more action. The day prior, the Ontario government had declared a state of emergency and the Ontario Premier had told protesters in Ottawa who had “held the city hostage for two weeks” to go home.63

The NSIA opened the February 12 meeting with a situation overview, noting that protest numbers were growing and that multiple ports of entry were experiencing blockages, with “slow roll” vehicle activity proving an effective protest tactic.64 The situation at the Ambassador bridge in Windsor was described as “very fluid” with law enforcement having begun taking some action. Protest activity in Ottawa was characterized as involving a significant escalation in “boldness,” with protesters increasingly harnessing social media across Canada. Following the NSIA’s situation report, various Cabinet Ministers, including the Public Safety Minister, the Minister of Transport, the Minister of Intergovernmental Affairs, Infrastructure and Communities and the Minister of Emergency Preparedness, all contributed remarks. The Minister of Public Safety (Mendicino) updated Cabinet on potential engagement with the leaders of the blockade, particularly in Ottawa. It was noted that engagement efforts by the Ontario government with protesters in Windsor had failed.

Minutes of the February 12 meeting included a detailed “IRG tracker” recording action items. This tracker document contains some revealing insights into the uses of intelligence for decision-making, including, as item #1, the fact that the NSIA would be charged with creating a daily situation report to “establish clear information sharing” and that a key Deputies committee, the Deputy Ministers committee on Operations (DMOC) would meet daily.65

The document also indicates that the Intelligence Assessment Secretariat at PCO, normally charged with the production of strategic intelligence assessments on global issues for the Prime Minister and Cabinet, would serve as the lead agency to pull together all intelligence reporting on the protests being produced across government agencies, including by CSIS and ITAC.
Intelligence on the protection of critical infrastructure, including at ports of entry, was charged to Public Safety, to “leverage existing information sources.” The document noted that an “evergreen list” of critical infrastructure was “in progress” with an especial need to identify critical infrastructure other than at ports of entry.

Preparing for invocation of the Emergencies Act, denoted as “track 2,” was clearly on the table, involving scenario planning “to show how bad things could actually get,” and the laying down of objectives and a tactical plan.

The final IRG meeting, prior to the decision to invoke the Emergencies Act, was held on late Sunday afternoon, February 13, 2022. It was followed on the evening of February 13, by a full meeting of Cabinet. The minutes of the February 13 IRG meeting are heavily redacted. The agenda for the meeting listed three items: progress on federal actions; a targeted situational update; and key communications. Nothing is readable regarding the situational update.

The associated IRG tracker indicated information was still sought on progress being made by PCO-IAS to bring all sources of intelligence together (“aggregation of intel”) and that this was to be presented at the February 13 meeting. The need to identify critical infrastructure other than at ports of entry was repeated. Planning for the possible invocation of the Emergencies Act was proceeding.

While the details of the situational update for the February 13 IRG were completely redacted, the NSIA did provide an update to the full Cabinet meeting on the evening of the 13th, parts of which were released. The agenda for the full Cabinet meeting contained, in addition to the situational update, two other items: an overview of the Emergencies Act; and an update on current activities/announcements for additional measures. The latter two agenda items were completely redacted. On February 14, a 33-page memorandum was prepared for Cabinet on “Invoking the Emergencies Act to End Nation-Wide protests and Blockades.” It is not available in the public domain.

The NSIA’s situational update for Cabinet, which followed immediately after opening remarks by the PM, indicated that multiple border points of entry continued to experience blockades, despite the success of law enforcement action to clear the blockade from the Windsor bridge. As Ms. Thomas, the NSIA, had done in previous IRG meetings, she highlighted the importance of social media use by the protesters for communications and organization. The threat picture regarding ideologically motivated violent extremism (IMVE) remained “stable and unchanged,” while CSIS continued to watch “persons of interest.” Ms. Thomas noted that recent law enforcement gains had been important and that the RCMP was taking enforcement action at the border crossing at Coutts, Alberta. Embedded in this sentence was a note by the NSIA that “there was a potential for a breakthrough in Ottawa, Ontario...” This statement became the headlines for media reporting as the documents were released by the Federal Court. Its meaning was elucidated in a statement from a spokesperson for the Public Safety Minister who was quoted as saying that:
“the potential for a breakthrough referred to negotiations led principally by the City of Ottawa with illegal blockaders in the days before the invocation of the Emergencies Act. The government closely monitored the status of negotiations, which were disavowed by many associated with the so-called freedom convoy and were ultimately unsuccessful.”

The NSIA subsequently told a conference in Ottawa on March 10 that the use of the Emergencies Act was justified because the Ottawa protesters were “dug in, they had supply chains, they had organization, they had funding coming in from across Canada, but also other countries” and “there’s no doubt they came to overthrow the government.” She indicated she was concerned about Canadian naivety regarding ideologically motivated extremism.

This partial glimpse into discussions and decision-making at the Cabinet level is revealing in important ways about the uses of intelligence at the political level during the protest crisis. Any conclusions must be tempered by the fact that the Cabinet record available in public is very incomplete. With that recognition, five observations can be made.

The first is that the federal government marshalled its highest level, collective discussions at the Cabinet table only late in the evolution of the “Freedom convoy” protests. Ministers were being individually briefed by senior officials, but the first meeting of the Incident Response group only occurred on February 10, two weeks after truck convoys converged on downtown Ottawa. The NSIA only began to compile her own situation report as of February 11. This late engagement may need to be re-considered when it comes to protest movements that may threaten national security and take on national dimensions, where an early federal government lead would clearly be important.

While there were delays in constituting the IRG, this should not be taken to mean that sub-Cabinet activity was not underway much earlier. A key missing narrative concerns the work of the Security and Intelligence Secretariat at the Privy Council Office, headed by an Assistant Secretary to the Cabinet, Mike MacDonald, who reported to the NSIA, as well as the discussions undertaken in the Assistant Deputy Minister committee on National Security Operations (ADM NS Ops). There is a revealing email sent by Mike MacDonald to the NSIA and other PCO officials on January 24, 2022, which indicated that the ADM NS Ops committee would begin meeting the following day. MacDonald told the NSIA: “Will let you know what the prevailing thinking is on the convoy issue and how we might structure ourselves if required. I would rather have structure and governance on this issue out of an abundance of caution than not.”

A limited set of “read-outs” from MacDonald to the NSIA, summarising ADM NS Ops meetings confirm the committee’s important role as both a coordinating body and a table where available intelligence could be digested. By January 26, the committee was already grappling with a key law enforcement and intelligence issue—trying to determine the “trigger” that would move the “Freedom Convoy” from a peaceful event to one requiring law enforcement action.” By February 2, the ADM NS Ops committee had been tasked by a Deputy Minister committee (DMOC) “to consider options and potential federal levers to manage the situation to resolution.”
Whatever thinking and action prevailed at this level of the federal bureaucracy it remains an open question whether it percolated, in a timely and full way, to the Cabinet table. Nor do we know what role intelligence reporting may have played in the decision to constitute the IRG on February 10

The second observation is that the government clearly struggled to find a way to bring together all the sources of intelligence available on the protest movement from different departments and agencies. There were multiple streams of threat reporting from different entities (ITAC, RCMP, Emergency Preparedness Secretariat and possibly others for which we lack public records). While they conveyed somewhat similar assessments of the “Freedom Convoy,” the very fact of multiple sources would not have been helpful to senior decision-makers. A need for a more integrated intelligence picture (“aggregate intel”) was clearly felt. The only surprise is this effort ultimately came to be led by the Intelligence Assessment Secretariat (IAS) of the Privy Council Office, which produces strategic intelligence assessment products for the Prime Minister and Cabinet on a range of global issues of importance. The IAS would not normally be a lead agency in reporting on domestic national security matters, a function within the mandate of both CSIS and ITAC.

There are possible explanations for the choice of the IAS as the Cabinet’s source of aggregate intelligence. These would include that the IAS reports directly to the NSIA, is embedded in a powerful central agency (PCO), has experience briefing the Cabinet and responding in a timely way to its informational needs, produces all-source intelligence assessments, and has a coordinating function across government for intelligence assessments. In addition, PCO-IAS might have been seen by senior decision-makers as a relatively neutral source, unencumbered by a mandate for domestic national security reporting focused on terrorism.

The IAS may simply have been seen as the best available option for intelligence integration as pressure mounted on the federal government to take action. It would, at the very least, have baseline knowledge-- in its normal reporting it would have had access to allied analysis on major protest events in other countries.

A third observation to be drawn from the Cabinet record is that the federal government did not have access to any granular picture of critical infrastructure across Canada and had to scramble to try to put one together. The most important and urgent need was to understand, as the IRG tracker suggests, key critical infrastructure vulnerabilities that might be targeted by the protesters, beyond the immediate border blockades. This was a reactive effort in the face of a lack of advance warning about the border blockades and an unclear picture of where protesters might strike next.

A data base of critical infrastructure, including vulnerability (or risk) assessments, should be part of any new critical infrastructure strategy being developed by the federal government. The existing critical infrastructure strategy (“National Strategy for Critical Infrastructure”) dates back to 2009 and is currently under review. The federal government continues a many-years-long effort to produce a national risk profile or register similar to that done by the UK.
government, but this has not been finalized. This work needs to be accelerated and brought to a conclusion, with both a classified and public version, as is the UK practice.  

A fourth observation is that the available picture of intelligence presented to Cabinet suggests that it operated at a high level of generality which may have been insufficient for truly informed decision-making. Intelligence is meant to provide a timely account of three dimensions presented by any perceived threat actor, whether state or non-state: intentions, capabilities and activities. Coming up with an actionable reading of any of these dimensions admittedly may be difficult.

With regard to the intentions of the protest movement and its leaders, the material presented to Cabinet (judging from the redacted record only) was almost non-existent. The Minister of Public Safety told the IRG on February 10 that they were seeing an “increase in systematic targeting and coordination” by “Freedom Convoy” leaders. No profiles of the leadership structure or personalities were mentioned in the redacted records. No indication of an intelligence picture of the protest movement’s aims was provided in the released version of the cabinet records.

On capabilities, the intelligence pictured conveyed to Cabinet was similarly very imprecise and not always coherent. Public Safety officials told the IRG on February 10 that, according to the lead OPP negotiator, “80% of protesters had a weak connection to the cause...” That same negotiator believed, rather optimistically, (and on unknown grounds), that “leaders of the protest could potentially be encouraged to leave and denounce the blockade in exchange for a commitment to register their message...” At the February 12 IRG, the Public Safety Minister provided a somewhat different picture, but still a very general one. He told his Cabinet colleagues that “there appear to be two distinct movements involved in the blockades. The first is relatively harmless and happy with a strong relationship to faith communities. The second is more concerning and comprised harder extremists trying to undermine government institutions and law enforcement.” No conclusion was drawn as to which movement might have the upper hand. Repeat statements by the NSIA made it clear that the government felt the protest movement was an adept user of social media to organize and fund-raise. Increasing reports of ex-military members advising and instructing the protests was noted and was clearly concerning. The RCMP commissioner told the IRG that her discussions with the OPS chief and the OPP commissioner indicated that the “mood on the ground has shifted to more hostility towards police.”

While it is understandable that the intentions of a grass-roots and factionalized protest movement may be difficult to divine, and may not be clearly known even to its leaders, the movement’s very reliance on social media platforms provided a potential opportunity for intelligence collection and assessment. The extent to which social media monitoring was a successful element of the overall intelligence picture presented to senior political decision-makers is an important issue but cannot be judged on the basis of the available Cabinet records. There is one fragmentary note in the redacted records that suggests impediments to the development of an intelligence picture based on social media. The IRG heard from the NSIA
on February 12 that “tracking social media does not fall into the mandates of the agencies involved in this issue.”

As far as can be discerned from the redacted Cabinet records, no capabilities assessment regarding the protest movement was ever presented. Any such capabilities assessment would have needed to combine elements of financial resources, foreign support or interference, protest numbers, leadership competencies, the demographics of the protest movement, the tactics used (including the tactical use of heavy equipment, “slow rolling,” and the deliberate presence of children in the protest blockades), social media capabilities and messaging, unity of purpose and factionalization, and the potential presence of weaponry, including any improvised devices.

The question of opportunities embedded in the intelligence picture for Cabinet mostly focused on prospects for negotiations, rather than on identifying vulnerabilities in the protest movement itself that could be exploited to resolve the crisis.

A revealing comment was made by the NSIA in a public forum on March 10. She argued that “we apply middle class values to things” and suggested that had there been a classic terrorist (religiously motivated violent extremist) element to the protest the reaction would have been very different. Ms. Thomas told her audience that Canada has a lot to “unpack” with regard to extremist protests and the threats they pose to democracy. The suggestion here is that there was some residual reluctance to fully appraise the national security threat posed by the “Freedom Convoy.”

A final observation concerns Cabinet governance of the national security and intelligence system. The IRG was pressed into service late in the evolution of the protest. It is a cabinet committee focused on managing emergencies, not on any more sustained strategic outlook and longer-term policy responses to the threat environment facing Canada. The circumstances of the protest, its extremist elements, its international implications in terms of blockages at the border, foreign funding, and impacts on Canada’s reputation with allies and adversaries strongly suggests the need for a dedicated, full-time cabinet committee on national security and intelligence. It may also point to the need for a more fundamental restructuring of national security and intelligence governance through the creation of a national security council along the lines utilised by the US and UK.

The National Security and Intelligence Adviser played a lead role, as appropriate to the office, in briefing the IRG and Cabinet, but that very role raises perennial questions about the authorities and influence possessed by the NSIA and whether these are adequate to ensure that the NSIA possesses a timely and coordinated intelligence picture that could be communicated to the PM and Cabinet, fully understood by senior political decision-makers, and able to be acted upon. Related to the authorities issues are perennial questions of resources and expertise within the Privy Council Office structure.
The National Security and Intelligence Adviser (NSIA)

The National Security and Intelligence Adviser to the Prime Minister (NSIA) occupies a pinnacle role in the Canadian national security and intelligence community. That role is not laid down in statute and has evolved since the creation of the office in 2003.

The National Security and Intelligence Adviser position was established in December 2003 (as the National Security Adviser) as part of a series of governance reforms to Canadian national security. The office was meant to be a more powerful version of the previous function of Security and Intelligence Coordinator at the Privy Council Office, which dated back to the 1980s. The first NSIA, Rob Wright, once described the new office as a ‘Security and Intelligence Coordinator on steroids.’ The brief description of the new office contained in the National Security Policy, released in April 2004, simply said that the purpose was to “improve coordination and integration of security efforts among government departments.”

In its 2018 framework report on the Government’s security and intelligence community, the National Security and Intelligence committee of Parliamentarians (NSICOP) identified the NSIA as a “core component”, because of “the important role the Advisor and his or her officials play in advising the Prime Minister and coordinating much of the security and intelligence community.” In addition to the advice to Cabinet and coordination function, exercised through membership on key deputy minister committees, such as the Deputy Ministry Committee on Operations (DMOC), the NSIA also serves as a principal channel for the flow of intelligence reporting to the Prime Minister and as a key coordinator for the setting of government intelligence priorities— the importance of which, the NSICOP report said, “cannot be overstated.” NSICOP also identifies a “challenge function” undertaken by the NSIA with the security and intelligence community. In terms of support for the NSIA, the Committee noted that two elements of the PCO reported directly to the NSIA: The Security and Intelligence Secretariat and the Intelligence Assessment Secretariat.

As part of the same annual report issued in 2018, the NSICOP also published a separate framework study on the government process for setting intelligence priorities. With regard to the NSIA’s stewardship over the intelligence priority process, the NSICOP made a series of recommendations designed to strengthen the leadership and managerial role of the NSIA, including with regard to the identification and implementation of Standing Intelligence Requirements (SIRs), which are key to ensuring that government-set general priorities are translated into operational missions.

NSICOP reports have opened up a small window on the role of the NSIA. Beyond its reporting, relatively little information is available in the public domain about the exercise of the NSIA’s authority, as important as it has become in the years since 2003.

It was not until 2014 that a National Security Adviser, then Stephen Rigby, first testified before a Parliamentary committee. No public address was given by any holder of the office until June 2021, when Vincent Rigby delivered a public speech hosted by the Centre for International...
Governance Innovation. External accountability has rarely been exercised, the sole instance being a special report undertaken by the National Security and Intelligence Committee of Parliamentarians regarding the role played by then NSIA, Daniel Jean, in dealing with concerns about foreign interference that emerged during the Prime Minister’s official visit to India in February 2018.

The most recent indication of aspects of the NSIA’s role was contained in a first-ever public address, delivered by the then NSIA, Vincent Rigby, to the Centre for International Governance Innovation in June 2021. He began by trying to explain what the NSIA actually does, understanding that few Canadians will have any awareness of the office. He noted that the NSIA provides “policy and operational advice as well as intelligence to the Prime Minister and Cabinet on issues related to national security.” He also mentioned his coordination role—“I help convene and coordinate the security and intelligence community,” to ensure “we work as one integrated team.” Mr. Rigby also emphasised the importance of his office in helping ensure decision-makers have access to the best possible intelligence, noting that “the case for intelligence has never been stronger” in order to understand the threats we face. The NSIA also plays an important role in liaising with international partners, especially in the Five Eyes intelligence partnership.

A relatively decentralised and siloed Canadian national security and intelligence system, needs to compensate for its governance architecture with a strong coordinating authority and connectivity with senior decision-makers across government—the raison d’etre behind the creation of the office nearly two decades ago. Whether the NSIA was able to fulfill this function in a consistent way, sufficiently early in the evolution of the “Freedom Convoy” protest cannot be determined from the public record. Seemingly ad-hoc decisions to have the NSIA responsible for compiling situational reports for Cabinet, and to have the Intelligence Assessment Secretariat that reports to her responsible for pulling together an integrated intelligence picture, suggests that there are lessons to be learned about strengthening the central governance of the national security and intelligence community and its responsiveness to public order emergencies.

The Canadian Security Intelligence Service (CSIS)

CSIS is Canada’s main intelligence agency charged with both domestic and foreign intelligence gathering, and analysis and advice to government on threats to the security of Canada. It is a civilian service created as a successor to the former RCMP security service in 1984, with its scope of lawful activities initially framed in the CSIS Act of that year.

The intelligence cycle for CSIS begins with establishing intelligence priorities and Service requirements. Setting CSIS intelligence priorities is part of a community-wide process
involving Ministers, and the National Security Intelligence Adviser. As part of this process the
Minister of Public Safety would provide a Ministerial Directive to the Service, which is then
translated into intelligence requirements by the CSIS Intelligence Assessments Branch. These
intelligence requirements are then operationalized according to three descending tiers, with
tier 1 requirements as fully resourced as possible, and tier 3 collection only when resources
allow. There is a further tier reserved for “watching briefs.” "99

CSIS intelligence collection is based on a variety of methods including OSINT, information
provided by members of the public, HUMINT (human sources managed by the Service),
information from foreign governments, especially Five Eyes partners, intelligence shared by
other Canadian government partners, and technical means used for surveillance and to
intercept communications, involving warrants authorised by the Federal Court. 100

The analysis component of the CSIS intelligence cycle involves two distinct entities. One is the
Intelligence Assessments branch (IAB), which is the CSIS centre of expertise for analysis of
threats to the security of Canada. It is paralleled by the CSIS-hosted Integrated Terrorism
Assessment Centre (ITAC), with a more focused mandate. ITAC’s known reporting on the
“Freedom Convoy” protests is discussed in a later section of this study. There is nothing in the
public domain about any relevant assessments that may have been produced by the IAB.

CSIS disseminates its intelligence reports primarily to the Government of Canada and Canadian
law enforcement agencies. Dissemination also occurs to global intelligence partners, especially
through the Five Eyes partnership. The key senior government of Canada clients for CSIS
reporting are the Minister for Public Safety, the Privy Council Office and Cabinet. 101

CSIS engages in a variety of intelligence missions including counter-espionage, foreign
interference, election security, cyber threats, counter-proliferation and guarding against insider
threats through security screening. Reporting on threats of serious violence to national security
is one of the key CSIS missions, with a majority of CSIS resources devoted to counter-terrorism
in the post 9/11 period.

Attention paid by CSIS to right-wing extremist threats has fluctuated over the past decade. A
review conducted by the Security and Intelligence Review Committee (SIRC) and reported to
the Minister in November 2017 charted the history of CSIS investigations of “Right-Wing
Extremism” (RWE) over the previous five years. 102 At that time CSIS included a basket of issues
in its investigations of right-wing extremism, including groups and individuals that espoused
racism, white supremacy, white nationalism, “white religion,” antisemitism, nativism, anti-
immigration, anti-government and anti-law enforcement, and homophobia. Also included were
a subset of groups that promote hate online.

The SIRC report noted that CSIS investigations of RWE were mainly event driven. CSIS
characterized RWE in the period from 2012 as “infrequent, generally unplanned and
opportunistic, and carried out by individuals rather than groups.” This outlook, and concerns
that most RWE activities were “near to” lawful protest, advocacy and dissent, which CSIS is
prohibited from investigating under s12 of the Act, as well as law enforcement attention to the issue, led CSIS to end its investigations of RWE in March 2016 on the grounds of lack of mandate authority and the absence of any value-added from such efforts, compared to police work. This decision was reversed following the shootings by a lone gunman at a Quebec City mosque in January 2017, which resulted in the deaths of six people, with a further five injured. 103

Since 2017, CSIS has devoted increasing resources to investigations of what it now calls “ideologically motivated violent extremism” (IMVE). The most recent CSIS annual public report for 2020-2021 (published in March 2022) noted that the IMVE threat is “complex and constantly evolving” and that since the beginning of the COVID-19 pandemic:

“IMVE activity has been fueled by an increase in extreme anti-authority and anti-government rhetoric often rooted in the weaponization of conspiracy theories. A number of Canadian influencers and proselytizers have emerged within IMVE movements. These IMVE influencers promote misinformation and action, including violence” 104

The same annual report gives short shrift to a distinct category of extremist threats, which CSIS now denotes as “politically motivated violent extremism,” and describes as “the use of violence to establish new political systems, or new structures and norms within existing systems.” Such investigations would be conducted under the CSIS Act s12, part d) mandate, usually referred to as subversion. The report simply noted that there were no PMVE-related attacks in Canada in 2021. 105

A third semantic category of violent extremism, often referred to as “Islamist terrorism” since the 9/11 attacks, is now labelled by the Service as “religiously motivated violent extremism” (RMVE) and continues to be a preoccupation of CSIS, although the threat is arguably greatly diminished from post-9/11 days. The 2020-21 annual report noted that “the ongoing threat of RMVE in Canada comes primarily from Daesh-inspired lone actors,” who operate without any direct connection or support from the Daesh movement that has lost considerable ground globally since the collapse of its so-called “caliphate” in the face of Western-supported military action in Iraq and Syria in 2016-2017. No RMVE-inspired attacks occurred in Canada in 2021. 106

A recent 2019 study by the National Security and Intelligence Review Agency (NSIRA) of investigations related to Canada-based extremists found significant ongoing problems in intelligence sharing between CSIS and the RCMP. NSIRA also noted the absence of any joint long-term strategy to address the threat. 107 It stated that, “on the whole, NSIRA found that CSIS and the RCMP have made little progress in addressing the threat under investigation.” 108 While key passages of the NSIRA study are redacted, it also clearly called attention to resource gaps in the CSIS intelligence collection program.

NSIRA’s study noted what it called a “fraught legal context” associated with CSIS’s human source collection problem, following a Federal Court finding in April 2018 that CSIS had used information derived from seemingly illegal activities in support of some of its warrant
These issues were addressed in Bill C-59, which provided CSIS with a new statutory framework for human source activities, with more checks and balances in terms of oversight by the Minister and by the new office of the Intelligence Commissioner.  

The NSIRA review also addresses ongoing challenges with the framework that governs CSIS-RCMP intelligence sharing, known as “One Vision 2.0” which was amended in 2015. Despite the various tools contained in the framework, NSIRA noted “a mutual reluctance to pursue the formal disclosure of information from CSIS, even in cases where the alleged threats were serious or imminent, and even though the alternative investigative path was slower and involved different challenges.” At the RCMP end, there were found to be trickle-down problems with CSIS-provided intelligence to regions, including INSETS, conducting investigations.

One of the most alarming findings of the NSIRA review was that by mid-2020, the RCMP was deprioritizing the investigation into right wing extremism and had admitted to CSIS that criminal charges remained “far off.” CSIS’s information was not making its way into the hands of RCMP investigators. NSIRA concluded on the state of the “intelligence-to-evidence” problem, that:

“Ultimately, CSIS and the RCMP appear to be trapped by the constraints that both organizations believe they must operate within in order to avoid compromising prosecutions.”

For the RCMP this means conducting independent investigations using evidentiary standards; for CSIS it means limiting any granular intelligence flow to the RCMP via advisory letters.

In an effort to tackle the problems and move beyond the limits of One Vision 2.0, CSIS and the RCMP jointly agreed to an independent study, called the “Operational Improvement Review,” (OIR) undertaken by an experienced security-cleared lawyer, Anil Kapoor. A final OIR report was delivered in March 2019. It called for significant changes to approaches to the intelligence-to-evidence problem to allow more robust sharing of intelligence by CSIS with the RCMP, including doing away with Advisory and Disclosure letters. The OIR final report also noted that “the strategic management of threats to national security requires a whole of government approach. This means there ought to be a consideration beyond the Service and the RCMP, of what action is in the broader public interest.” It argued that whole-of-government strategic discussions could be handled by the current ADM committee on national security operations.

Finally, of relevance to this study, the OIR report argued for the RCMP to adjust its approach to national security investigations by devoting more effort to investigations in the “pre-crime” space and giving greater attention to counter-radicalisation efforts.

NSIRA saluted the OIR final report as “complex, ambitious and a promising effort to address longstanding problems that have hindered Canada’s ability to prosecute or otherwise address threats to national security.” It also believed that implementation of the OIR would be challenging. In response to the NSIRA recommendations CSIS and the RCMP noted that the OIR contained 76 recommendations. They committed to implementing them and creating a
new “One Vision 3.0” framework for intelligence sharing. But CSIS and the RCMP also noted that “this complex work...is ongoing and challenges remain.” 114

What progress had been made in the report’s implementation by the time the “Freedom Convoy” took to the road, is unknown.

CSIS and the RCMP did not directly respond to the NSIRA recommendation on the need for a joint, long-term strategy to deal with investigations into extremist threats, nor did they directly address resource constraints. 115

Another recent NSIRA review looked at a technical capability employed to support open-source intelligence—the use of geolocation. This review was prompted by a Federal court decision in September 2017 (the “IMSI decision”) which found that it was lawful for CSIS to obtain, under its section 12 authority, geolocation information for which there is a low expectation of privacy—e.g. subscriber information and device number—but reaching beyond that for the actual location of an individual as pinpointed by their mobile device would require a warrant. The NSIRA review is heavily redacted but it is clear that CSIS examined legal issues around the collection of geolocation data in preparation for a pilot project in early 2018 but was prepared to push ahead. Eventually a formal legal opinion was provided to the Service that provided for a narrow window for use of geolocation data collection without a warrant. In general, the NSIRA review found that new technologies for data collection combined with a “fluid” legal situation created high legal risks for the Service which would need to be better managed. 116

The challenges associated with ramping up intelligence collection against IMVE threats, with information sharing with the RCMP, and with technological adaptation, are compounded by long-running public criticisms of the methods employed by the Service in monitoring protest movements.

CSIS and protest monitoring:

The Service has been locked in a long battle with a Canadian civil liberties NGO, the British Columbia Civil Liberties Association (BCCLA) over allegations made by the BCCLA, beginning in 2014, that CSIS had illegally spied on pipeline protestors (who opposed the Northern Gateway Pipelines project—subsequently abandoned following an adverse environmental assessment). The BCCLA concerns were rooted initially in a news story based on access to information records. The BCCLA allegations were set out as a complaint to the Security Intelligence Review Committee, CSIS’s external review agency at the time. 117 SIRC engaged in a lengthy complaint investigation, and eventually rendered a decision in September 2017.

SIRC found that CSIS had not engaged in intelligence collection against lawful advocacy, protest or dissent and thus had not contravened section 12 limitations. It noted that SIRC had kept a “watchful eye” on this area as it related to CSIS operations and had found in reviews dating back to 2002-2003 that CSIS’s conduct in monitoring protests had been found to be appropriate. However, the SIRC report understood that there was a perceptual issue about
Spying that the Service needed to acknowledge and encouraged CSIS to hold “inclusive public
discussions with the groups involved in the present complaint.”

The BCCLA did not accept the SIRC ruling on its complaint and has appealed the ruling to the
Federal Court. It also appealed the SIRC order sealing the evidence presented in the case, and
won a ruling from the Federal Court that it could make the records of the case provided to
BCCLA in redacted form, totalling over 2200 pages, public. BCCLA then proceeded to publish
these records in 19 volumes on its website, under the heading of “The Protest Papers.” BCCLA
rejected the SIRC argument that CSIS could legitimately investigate specific targets associated
with environmental protests, and also believed that information collected incidentally or for
what the Service referred to as “domain awareness” was offside. As the BCCLA stated: “we
believe that this amounts to keeping tabs on peaceful environmental groups, which is not only
unlawful under the CSIS Act, it suggests a bias in the spy agency that sees environmentalists as
an inherent threat.”

While CSIS witnesses before SIRC upheld the lawfulness of CSIS’s behaviour, it is difficult to
measure the extent to which public suspicions of CSIS spying may negatively impact on the
Service’s own investigations, as CSIS is aware that it requires social licence to function
effectively. As a recent CSIS online publication devoted to the IMVE threat put it, “CSIS is
committed to establishing itself as a trusted partner for Canadian communities and to building
those partnerships through dialogue, mutual respect and reciprocal action.” It is difficult to
do this if some proportion of Canadians feel CSIS is spying on them without reason.

While there is currently no public access to CSIS reports on the “Freedom Convoy”
demonstration, unlike material now available on ITAC reporting, indications of the Service’s
general engagement can be found in two sources.

One source involves two public speeches delivered by the CSIS Director, David Vigneault, which
brace the protest movement. Both speeches call attention to the rising threat posed by IMVE
and link its acceleration in part to the COVID-19 pandemic and associated conspiracy theories,
online hate, and anti-government rhetoric. In February 2021, Mr. Vigneault stated that “while
violent extremism remains an ongoing threat to our safety and a significant preoccupation for
CSIS, the greatest strategic threat to Canada’s national security comes from hostile activities by
foreign states.” He referenced spying, cyber attacks, data theft, economic attacks, the
targeting of Canadian research, foreign interference, and insider threats.

In the speech the CSIS Director delivered in May 2022, following the law enforcement shut-
down of the “Freedom Convoy” protest, Mr. Vigneault gave greater emphasis to the IMVE
threat, noting that it is constantly evolving, “fuelled by extreme views around race, gender,
power and authority.” He told his University of British Columbia audience that CSIS continues to
increase its resources dedicated to investigations of IMVE, while also indicating that “we need
to understand threats in an international context,” and cannot ignore the world outside our
borders.
Therein lies a new dilemma for CSIS, how best to balance investigations of domestic threats to national security, with international ones. This dilemma is further extended by a problem that CSIS has not been shy to raise in recent months—the limitations of the CSIS Act.

The CSIS Director stated in February 2021 that the CSIS Act was better suited to the threats of the Cold War Era and now “greatly impedes our ability to use modern tools, and assess data and information. We need laws that enable these types of data driven investigations, carefully constructed to reflect the values we share in our democracy, including assurances of robust privacy protections.”

A similar message was conveyed in the CSIS annual Public Report for 2021, making a direct pitch for a comprehensive review of the CSIS Act, which “has not adequately evolved to meet the challenges of today’s complex global threat environment.”

Whether and how this inadequate evolution of the CSIS Act might have affected its reporting on the “Freedom Convoy” protests in early 2022 can only be determined by access to confidential records.

There are breadcrumb clues in the testimony that the CSIS Director provided to a joint parliamentary special committee in its study of the exercise of the Emergencies Act. Mr. Vigneault affirmed the material included in ITAC reporting, to the effect that CSIS was looking at specific targets of which it was previously aware, that it focused attention on IMVE proponents seizing on the protest movement to recruit and radicalise it, and that it worried about lone actors. CSIS provided intelligence to law enforcement partners through a “joint intelligence group (likely a reference to the RCMP’s National Security Joint Operations Centre (NSJOC)) and also informed the government.

The most revealing statement made by the CSIS director came in a question from Senator Harder. Mr. Vigneault told the Committee that CSIS was providing “sometimes very definitive views,” but qualified this by saying “but it’s also clear that what we saw and what we knew then was fluid. We did not have the full picture. That added to the level of uncertainty that everybody we were working with was feeling about how this very volatile demonstration was evolving. I think these would be some of the elements that we would want to make sure the Governor in Council would have been aware of while making the decision to invoke or not the Emergencies Act.”

This seems the crux of the matter when it comes to understanding the nature of CSIS intelligence reporting on the “Freedom Convoy.” There was a mixture of fluidity and volatility in the makeup of the protests; there was no full intelligence picture; there was a widely shared sense of uncertainty about what might happen next. All may have contributed to the decision to use the Emergencies Act. There is a direct link in one of the conditions stated by the Governor in Council to support the invocation of the Act, namely:
The potential “for an increase in the level of unrest and violence that would further threaten the safety and security of Canada.”

That there was a lack of a “full intelligence picture” is a significant admission. But it also must be acknowledged that intelligence services never have a “full picture.” What seems clear in the case of the intelligence assessment of the “Freedom Convoy” is that it was not just partial but that there was a lack of confidence in its findings as a guide to what the future might hold. Left uncertain, the Government may have felt compelled to reach for the powers of the Emergencies Act as a last resort.

Minister Blair in later testimony to the committee put a somewhat different construction on the intelligence picture. He referred on more than one occasion to “strong intelligence” about the intentions of those taking part in border blockades to either return to blockades that had been cleared by law enforcement or take their fight to new border crossing points. He said that the government did not want to play “whack a mole” with the border blockades “and we wanted to make sure that we ended that threat conclusively and forever.” When pressed by a NDP member of the committee about “strong intelligence” documentation on the intentions of protestors involved in the border blockades, Mr. Blair said he was orally briefed on the matter and “read a number of open source reports.” But he also shifted his language from “strong intelligence,” to “a very sincere, legitimate concern that these blockades would return...” Normally, we would assume a difference between “strong” intelligence, based on assessed reporting, and “concern.”

The question that emerges from this testimony is whether the government possessed “strong intelligence,” (Minister Blair) on the intentions of “Freedom Convoy” protestors, or only an incomplete intelligence picture (CSIS Director Vigneault) in which it lacked full confidence. It cannot be both.

**The Integrated Terrorism Assessment Centre (ITAC)**

A key to a deeper understanding of the nature of CSIS threat reporting, and a confirmation of the extent to which that reporting was never able to generate a holistic (“full”) intelligence picture, can be found in the work of the CSIS-hosted Integrated Terrorism Assessment Centre.

The Integrated Terrorism Assessment Centre is an intelligence fusion centre housed in CSIS. It serves as a government-wide resource and as an asset for the National Security and Intelligence Adviser. The Centre was first created in 2003. Its function was announced and highlighted in the Government’s National Security Policy in 2004.
The National Security Policy noted that the creation of what was then called the Integrated Threat Assessment Centre, mirrored that of post-9/11 units established by our close Five Eyes partners, including the UK’s Joint Threat Assessment Centre. The new Canadian centre would be staffed by representatives drawn from a broad range of departments and agencies, to help ensure that organizational silos in intelligence reporting would be broken down. Prior to the creation of ITAC, the national security policy noted that “there has been no comprehensive and timely central government assessment that brings together intelligence about potential threats from a wide range of sources to allow better and more integrated decision-making.”\textsuperscript{133} The new centre’s remit was thus ambitiously framed:

\textit{“The centre will do a comprehensive analysis of all available information on potential threats to Canada and make the results of that analysis available to all who require them.”}\textsuperscript{134}

This ambitious agenda proved difficult to realize. Staffing was an issue from the outset, with departments and agencies not always willing to lose analytical talent to the new body. Reporting frameworks and channels had to be created. ITAC had to build a reputation for quality reporting, which was often hampered by a view that it was overly reliant on open-source intelligence and tended to mirror media reporting. Difficult decisions had to be made about the nature of distribution of ITAC’s reporting and associated levels of classification. If it tried to reach a wide range of first-responders at both the federal, provincial and territorial, and municipal levels, it could only do so with low levels of security classification for its reports, which may have also harmed its reputation within the intelligence community.\textsuperscript{135}

The greatest unmet ambition for ITAC was that it was never able to embrace a mission to conduct integrated threat assessments on a wide range of issues. The stimulus for this larger mission was in part derived from the experience of the SARS outbreak in Canada in 2003 and a realization of the gaps that existed between public health security and national security. The National Security Policy, in its chapter on Public Health Emergencies noted that:

\textit{“Going forward, the Government intends to take all necessary measures to fully integrate its approach to public health emergencies with the national security agenda...the public health dimension will figure prominently in the Government’s integrated threat assessments.”}\textsuperscript{136}

No such development occurred at any time in the evolution of ITAC, including with regard to the outbreak of COVID-19 in 2020.

The reasons for this were various—resource constraints; leadership challenges; the absence of an identifiable government readership for wide-ranging threat assessments; and the fact that ITAC was housed at CSIS, reported to CSIS for management issues, and was inevitably drawn into the orbit of CSIS’s mandate activities. The brief description of ITAC on the Government of Canada’s website notes that it “operates under the provisions and authorities of the CSIS Act,” which would include the Act’s definition of threats to the security of Canada at s2.\textsuperscript{137}
Over time ITAC was renamed and refocused, becoming the Integrated Terrorism Assessment Centre in 2011, reflecting an over-riding concern with terrorist threats in the years after 9/11. It operates today as such, with the original wider-scope ambition long-forgotten. One commentator, former CSIS analyst Stephanie Carvin, notes that ITAC has little transparency, and an unclear mandate. She also argues that some of its reporting on protest movements attracted controversy over the years. Her conclusion is worthy of note: “it seems clear that fifteen years after its founding, ITAC continues to struggle to find its place in the Canadian national security architecture.”

ITAC reporting on the “Freedom Convoy” was centred on the possibility of threats emanating from ideologically motivated violent extremism (IMVE), which fell directly under the Centre’s mandate for reporting on terrorism-related issues. Possible violence stemming from civil unrest was seen as a police matter, not within ITAC’s mandate. But this distinction proved challenging for intelligence coverage of the “Freedom Convoy.”

Some classified ITAC threat reporting on the “Freedom Convoy” protest movement was leaked to reporter Justin Ling and included in an article Ling published with the Guardian newspaper. This led to an unsuccessful effort by ITAC to identify the source of the leak.

More recently, an Access to Information request has led to the release of a tranche of ITAC reporting on the protest, including the material leaked to Ling. The release was in response to an ATIP request for intelligence reports, intelligence studies and intelligence briefs on protests in Ottawa and at Canada-US border crossings against COVID-19 measures. The released material responsive to this request includes eleven ITAC reports related to the “Freedom Convoy” protests, issued between January 26 and February 24, 2022. It does not include any reporting undertaken by the CSIS’s Intelligence Assessment Branch or any reports generated by CSIS’s open source centre. In their totality, they may not represent all the reporting undertaken by CSIS, but the ITAC material, even with redactions, provides an important insight into the nature of its intelligence contribution during the protests.

The very first ITAC threat assessment was published on January 26, under the title “Possibility of IMVE-driven opportunistic violence on the margins of truck convoy protest.” The threat assessment is redacted almost in its entirety, but was at least timely in noting that the protest truck convoy was expected to arrive in Ottawa on January 28-29.

This first ITAC report was followed by a series with a similar emphasis on the potential for violence stemming from IMVE online rhetoric, swirling around the protest convoy, and the physical presence of some IMVE threat actors and conspiracy theorists in the convoy movement. ITAC foresaw a possible violent clash between extremists and law enforcement as the protest movement arrived in Ottawa, but also was at pains to distinguish between legitimate protest actions, which it initially believed the convoy organizers embraced, and those who might be driven to extremist violence. In a second report on January 27, ITAC noted that the resumption of Parliament on January 31 could motivate a “dedicated group of protesters to prolong their protest in Ottawa and/or seek interaction with Canadian politicians.”
indication was supported by the reproduction of a “Permanent Gridlock zone” map originally circulated on 4Chan on January 27. 146

The ITAC reports of January 26-27 can be usefully compared with public announcements made by the Ottawa Police Service (OPS). The OPS briefings were a form of public intelligence, discussed in a later section of this report, and signalled the Ottawa police assessment of the threat posed by the “Freedom Convoy.”

In a media briefing on January 28, as the first convoy of trucks arrived in Ottawa, OPS Chief Peter Sloly stated that:

“the demonstrations this weekend will be unique, fluid, risky and significant. These demonstrations are national in scope, massive in scale, polarizing in nature and come almost two full years into a highly stressful and tragic global pandemic.” 147

Chief Sloly noted that while the OPS had been in touch with protest organizers and that they had indicated they will engage in peaceful demonstrations, he also stressed that there were many “parallel” demonstrators that the police had not been able to engage with, and social media actors domestically, nationally and internationally “who may or may not come to the demonstrations but who are inciting hate, violence and criminality.”

Chief Sloly was also candid about what the OPS did not know. They did not have a fix on the number of trucks to descend on Ottawa or the number of demonstrators. They did not know when the demonstrations might end—suggesting that they could go into the following week.

The OPS chief also indicated on January 28 that the Ottawa police were employing ‘intelligence-led policing’ approaches, stating that the OPS had been meeting with its partners to develop an operational plan “to ensure that we have the most current information and intelligence from all sources. This intelligence will inform the spectrum of risks, threats and variables.” 148

Analysis of OPS intelligence is beyond the scope of this report, as is the operational plan that was deployed to meet the Freedom Convoy protest in Ottawa, which was heavily criticized. But is notable that the intelligence picture available to the OPS, at least that part of it conveyed in public, shared common elements with that of ITAC and in some respects exceeded ITAC reporting in its early depiction of the dynamics of the “Freedom Convoy” protest.

Further ITAC reporting on February 3 continued the assessment of possible “opportunistic, low-level violence,” in the days ahead fueled by several factors: the “potential” presence of IMVE adherents; protester frustrations; and citizen counter-protest and action. 149 This assessment was repeated following the second weekend of the truck convoy presence in Ottawa and demonstrations across the country. It noted a shift away from the original focus on supporting truckers contesting government COVID-19 vaccination policies to a wider protest umbrella featuring “various groups opposing public health measures.” 150 The ITAC threat assessment
update on February 7 noted that some 7,000 people had been engaged in protests and counterprotests over the previous weekend in Ottawa. The protest activity was deemed “relatively peaceful” but concern was expressed about violent online rhetoric and the physical presence of ideological extremists at some demonstration. 151

Again, the ITAC reporting can be compared to OPS media briefings assessing the threat posed by the “Freedom Convoy.” On Friday, February 4, as the second weekend of protest activity began in Ottawa, The OPS chief stated that the police would begin a surge and contain strategy. He noted that downtown Ottawa residents had been “severely impacted by unlawful acts. Including harassment, mischief, hate crimes and noise violations. He noted that intelligence gathering efforts were being stepped up by national, provincial and local law enforcement agencies and that these efforts would support evidence-gathering for criminal prosecutions. Chief Sloly admitted that the “current occupation” of the Parliamentary precinct remained unresolved. He characterised the demonstrators in the “red zone” as “highly organized, well-funded and extremely committed to resisting efforts to end the demonstration safely.” This remains, the OPS chief stated, “a very violative and very dangerous situation.” 152 In its public pronouncements, the OPS demonstrated, once again, that it was ahead of ITAC in depicting the nature of the “Freedom Convoy” threat.

As the third weekend of convoy protests approached, ITAC sounded one new note in its threat reporting on February 10. It now worried that IMVE adherents “may feel empowered by the level of disorder resulting from the protests.”153 This would have been old news to the Ottawa Police Service. It also noted increasing online violent rhetoric responding to enforcement actions or threats of action by the Ottawa Police Service—these included a suggestion for protesters to collect the personal information of law enforcement officers and politicians supporting the OPS measures. A “corrected” but very similar version issued the following day represented the last ITAC threat reporting produced prior to the weekend meetings of the Cabinet Incident Response Group and the government’s decision to invoke the Emergencies Act on February 14. 154

At the same time that ITAC was concluding its series of threat assessments prior to the invocation of the Emergencies Act, the OPS held a further media briefing on February 10. Chief Sloly began by referring to his efforts to secure additional resources from federal and provincial partners to deal with an unlawful occupation, a matter to which he gave repeated emphasis and which he said was essential to deal with the protest. The OPP was taking the lead in trying to coordinate additional police resources that could flow to Ottawa. Hate crimes were being investigated and arrests had been made. Chief Sloly urged additional protestors not to come to Ottawa on the weekend and warned against unlawful activities. He noted that 400 trucks remained in the red zone and that at least one major tow truck operator had been threatened; other operators were proving to be uncooperative. Asked about the involvement of former military and police personnel in the demonstration he emphasised what he called the unprecedented capability of the protest movement, which posed a significant risk. 155
Following the lifting of the Emergencies Act on February 23, ITAC issued a report the following day with the melancholy observation that:

“Supporters of IMVE will continue to encourage and capitalize on, anti-government sentiments and protest movements, whether related to the pandemic or other issues, in an attempt to degrade public confidence and social cohesion, and to attract vulnerable individuals to their ideological cause.” 156

ITAC believed IMVE threats would persist “into the foreseeable future.”157

Several things are worth noting about the series of ITAC reports. One is their sheer generality. They consistently pointed to possible outcomes only. More precise predictions about the dynamics of the protest movement were missing. Even levels of confidence in their observations were not indicated—at least in the redacted pages. The only exception was in the repeated finding that a “coordinated, complex” terrorist attack arising from the “Freedom Convoy” was unlikely. The inability to produce more “actionable,” as opposed to contextual, intelligence would presumably have lessened the value of these reports for decision-makers and would not have helped in ensuring the receptivity of decision-makers to ITAC reports.

A second point is that the ITAC reporting did not deliver any holistic picture of the protest movement, its leadership, its constituents, or its stated objectives. ITAC was more narrowly focused on any IMVE element, either in terms of online rhetoric or the presence of known IMVE actors and anti-government conspiracy theorists in the protest camp. This was an important focus and clearly within ITAC’s mandate and that of its host, CSIS. But built into this assessment lens may have been a tendency to assume that other, less examined, elements of the protest movement were engaged in lawful democratic protest and somehow did not share the anti-government/anti-authority sentiments rampant among IMVE ideologues. A bifurcated approach to the protest movement, separating out possible IMVE elements from others was an artificial construct, not least given the ITAC observation that IMVE incitement might trigger opportunistic violence by individual (“lone”) protestors or that IMVE influencers might find ways to mobilize the larger protest movement to violence by exploiting protester frustrations and capitalizing on the dissemination of conspiracy theories.

A third observation is that at no time was ITAC able to predict or comment on the border blockade tactics developed by the “Freedom Convoy.” Its threat metrics did not include threats to critical infrastructure. On the protest at Coutts, Alberta, it simply commented on February 7 that “the size of the protest has ebbed and flowed over the last ten days. And there is no information to suggest the organizers intend to end the protest.”158 The Coutts border blockade would emerge as one of the most dangerous flash points during the “Freedom Convoy” protests. An ITAC threat assessment issued on February 17, days after arrests had been made at Coutts and weaponry and body armour seized, astonishingly made no reference to these developments despite widespread media coverage. 159
There was no reporting from ITAC on the border blockade at the Ambassador Bridge (at least in the released material) or at other sites (Emerson, Manitoba, and the Pacific highway in B.C.) Comparisons between known ITAC threat assessments and information made publicly available by the Ottawa Police Service suggest that the OPS had, from the outset, a better overall appreciation of the threat posed by the “Freedom Convoy” movement, even while its policing operations were overwhelmed by the size, volatility, and duration of the protests in the downtown Ottawa core.

ITAC operated in a narrow groove. This may explain, in part, the late determination of the Cabinet Incident Response Group to turn to the Intelligence Assessment Secretariat at PCO for a more integrated intelligence picture. But it is also a comment on the extent to which ITAC had drifted away from the original vision behind its creation in 2003-04.

A recent independent report on Canadian national security, published in May 2022, made the interesting recommendation that ITAC should be moved from CSIS and merged with the Intelligence Assessment Secretariat at PCO, to report to the NSIA. The rationale for this recommendation was not rooted overtly in the intelligence assessment challenges posed by the Freedom Convoy protest, but instead referenced the need for a strong, central assessment unit that could also serve a coordinating function for assessment across the government of Canada and help strengthen “the coherence of the intelligence cycle as a whole.” This sounds like a reincarnation of the original vision for ITAC, and may be made all the more necessary by the experiences of the “Freedom Convoy” protests.

The Royal Canadian Mounted Police (RCMP)

Alongside CSIS and ITAC, the RCMP played a key role in advising the government on potential national security threats posed by the “Freedom Convoy,” a role that stemmed from its mandate to investigate and prevent national security criminal activities. This mandate is conducted under the RCMP’s federal policing program, with oversight and coordination provided by the Federal Policing National Security unit at RCMP headquarters in Ottawa, headed by an Assistant Commissioner. Investigations themselves are conducted by teams in the RCMP’s regional divisions, some of which have Integrated National Security Enforcement Teams (INSETS). There are INSETS in Ottawa (National Division) in Ontario (O division, based in Toronto), and in Alberta (K Division based in Calgary), for example.

As noted earlier, the RCMP manages intelligence sharing with CSIS, a key partner, in accordance with a framework doctrine called “One Vision 2.0,” now under review. A redacted reference to RCMP-CSIS relations in talking points prepared for the NSIA for a Deputy Ministers’ meeting on February 9, simply states that: “RCMP remains well connected with CSIS.” How effectively intelligence sharing was managed between the two agencies during the “Freedom Convoy” protests cannot be assessed on the basis of the available evidence, but it is unlikely that deep-rooted problems were fully surmounted.
A selection of RCMP threat reporting has become available through an Access to Information Request. It may not represent a complete picture of the intelligence perspective of the RCMP, but it suggests RCMP threat assessments replicated the same deficiencies as the ITAC reports in their generality and inability to provide any foresight analysis.

Details of the distribution of this RCMP threat reporting are unavailable. According to testimony provided by Commissioner Lucki on May 10 to the Special Committee on the Declaration of Emergency 2022, the RCMP provided situational reports throughout the duration of the “Freedom Convoy” protest; these were given to the Privy Council Office, who she described as “the keepers and distributors of all information regarding this event.”

The RCMP reports on the “Freedom Convoy” were generated by the “Ideologically Motivated Criminal Intelligence Team,” (IMCIT) within the RCMP’s Federal Policing National Intelligence. The team produced special threat advisories on the “Freedom Convoy” beginning on January 25 and running till at least February 11, 2022. These advisories were circulated with a low security classification ("Protected A"), relied almost exclusively on open source intelligence, which they documented, and were designed, according to the team, “to provide situational awareness of threats to public order, public safety and the security of public officials arising from violent online rhetoric opposing new and ongoing public health restrictions.” Situational awareness by the RCMP was basically a form of current intelligence reporting.

The starting point for the threat advisories was a series of unknowns—regarding numbers of vehicles and protestors associated with the “Freedom Convoy,” the likely targets of their Ottawa protest, and the uses of funds raised online. A consistent feature of the reporting from January 25 identified IMVE actors as part of the convoy movement but no determination was made about the likelihood of IMVE action. IMCIT reporting soon added another important unknown—how long the protestors might remain encamped in Ottawa.

From the outset the IMCIT threat advisories painted a picture of an extremely diverse protest movement, ranging from those who had experienced “hardship” due to COVID-19, to ideologues who sought participation in the “Freedom Convoy” to “further their narratives.” Within the latter group, the RCMP team believed that there was a “diversity of views” regarding the use of violence. IMCIT was particularly interested, as it observed the social dynamics of the protest movement through the lens of social media, to determine its attitude to law enforcement.

The intentions behind the “Freedom Convoy” protest remained a mystery to IMCIT even as trucks began to arrive in Ottawa. The presence of heavy machinery on some of the transport trucks headed to Ottawa was regarded as a puzzle. The IMCIT simply noted that “it is possible it will be used to obstruct areas.” An online post, complete with photograph, that referred to a “Freedom Convoy” helicopter and a drone pilot embedded with the protest (accuracy unknown) may have sparked a decision to issue a “NOTAM” closing access to airspace over a large swath of downtown Ottawa.
Past the first weekend of the “Freedom Convoy” encampment in downtown Ottawa, IMCIT tried to look ahead, but their OSINT sources provided little direct help—“there is limited information posted about formal activities planned for the coming week.” The RCMP team did note online information indicating that some protestors intended to stay until public health restrictions and vaccine mandates had been removed, but offered no assessment of the likelihood of this protest development. 170

ICMIT noted solidarity actions in every province of Canada and offered a pessimistic outlook on the potential impact of law enforcement efforts, stating that action at any one event “will likely be perceived negatively and may spark more solidarity activities or adverse behaviour elsewhere.” 171

Inexplicably, IMCIT took a one week break, between February 3 and February 10, from its threat advisory reporting. In its last available update prior to the invocation of the Emergencies Act, the RCMP team posted its longest report yet. By February 10 it was prepared to conclude from its OSINT sources that the protesters had no intention of leaving Ottawa. Even then IMCIT was uncertain whether the protest movement might be satisfied with meeting with government representatives or would pursue maximalist aims to force all public health restrictions to be lifted. This uncertainty was reinforced by an emerging belief that there was no real “central leadership” to the Ottawa protests. 172

IMCIT also now took notice, for the first time, of the fact that convoy supporters formerly employed in law enforcement and the military were associated with the convoy organizers. The concern was that their knowledge of policing tactics and techniques might be deployed by the “Freedom Convoy” to counter law enforcement actions. Added to this was a speculative fear of the potential for “serious insider threats” on the part of serving members of law enforcement and the military. As the threat advisory put it:

“Those who have not lost their jobs, but are sympathetic to the movement and their former colleagues, may be in a position to share law enforcement or military information to the convoy protesters.” 173

This was a striking claim. The basis for it is unknown. What we do know is that by February 10, the IMCIT was liaising with RCMP Divisional Criminal Analysis units across Canada and feeding their reports into a picture of nation-wide “solidarity actions.”

The bright line for any form of intelligence reporting involves straying across the boundary between presenting situational information to inform policy-making and using intelligence to lead policy-making in some desired direction. IMCIT reporting did not cross any bright lines, and probably did not have the power or influence to do so, but neither was it helpful in assessing the intentions, capabilities or anticipated future directions of the “Freedom Convoy.” Its repeated note of pessimism about the likely blowback from any law enforcement actions in the face of what it described as a nation-wide movement is striking. Nor was IMCIT ever prepared
to pronounce in any decisive way on the ideological make-up of the “Freedom Convoy.” Its February 10 portrait was little changed from that offered in its first report on January 25:

“IMCIT assesses that this protest has attracted both in-person and online support of individuals with a variety of grievances, some ideological in nature and others who may have experienced personal hardships due to COVID-19 or are experiencing pandemic fatigue. Overall there is anti-government sentiment based on the fact that the protesters want public health restrictions lifted and the government has the power to do so. However, not all individuals who may hold anti-government views on the specific topic of public health restrictions are believed to support extreme activities and there are diverse views regarding the use of violence during the convoy.”

There are different ways to read this determinedly even-handed assessment. It may, simply, be a realistic portrait; it may be far too sympathetic. What is clear is that the IMCIT threat advisories maintained a relatively unchanged picture of the makeup of the protest movement from the inception of its reporting and were unable to successfully capture any dynamic changes.

The threat reporting produced by the RCMP team reflects two perils. One is an inability to treat open source intelligence as other than a large and diverse assemblage of information from which no conclusions can be drawn. OSINT on a target may even lead to distorted perceptions influenced by the contents of social media messaging, if not properly assessed—a form of ‘drinking the kool-aid.’ The second peril concerns the absence of any value-added to such intelligence reporting, despite drawing, as it did, on the best available source of information about the “Freedom Convoy.”

The RCMP was no better placed than its intelligence partners in offering any early warning in the form of actionable intelligence on “Freedom Convoy” developments in general. But in one specific case, an RCMP INSET investigation, drawing on a variety of investigative tools, was able to arrest a group of individuals associated with the border blockade at Coutts, Alberta and in particular involved in providing security for the protesters. Members of this “sub-group” as they were defined in court-redacted warrant applications, had transported weapons and body armour to a site near the blockade. They were arrested on the evening of February 13 and the morning of February 14, 2022 and charged by the RCMP with conspiracy to murder, following a search of three trailers. Among the material seized, in addition to lethal weaponry, was a body-armour vest with a “Diagolon” patch. Diagolon is a far-right organization whose activities have been analysed by the Canadian Anti-Hate Network. The network has identified two of the individuals arrested at Coutts as having prior links to Diagolon.

As the court warrant applications indicate, not only did the RCMP insert two undercover officers into the group, who provided crucial intelligence on the organization and leadership of the protest, and on a weapons smuggling scheme, but they used other intelligence gathering techniques, including social media searches and emergency wiretaps. CSIS membership in the Alberta INSET based out of Calgary indicates their likely involvement in some form in
intelligence gathering on the Coutts blockade. The ability to successful deploy RCMP undercover operatives, both female, into the protest group, suggests a longer term and ongoing investigation into the IMVE threat that was presented at Coutts and may be a striking indication of at least one investigative success in the face of threatening developments presented by elements of the “Freedom Convoy.”

Whether RCMP or other agency reporting of these developments at Coutts, coming as they did just prior to the invocation of the Emergencies Act, had any decisive impact on the government’s decision cannot be determined on the basis of the available evidence. As noted above, ITAC, as one key channel of threat reporting, does not seem to have been focused on them. Its gaze may have been Ottawa-centric.

RCMP intelligence work was meant to be enhanced with a key initiative begun in 2014, the creation of the National Security Joint Operations Centre. NSIJOC was established as an inter-agency fusion centre to deal with threats posed by terrorism and high-risk travellers, taking its initial inspiration from the experience of the October 2014 terrorist attacks on Parliament Hill and in Quebec. Membership of the NSIJOC grew to include representatives from RCMP, CBSA, CSIS, IRCC, DND, FINTRAC, CSE, GAC and the CRA by 2017. The NSIJOC was meant to be a centre of expertise on national security investigations, to share information and intelligence among its partners, and to help coordinate a whole of government response to “emerging issues.” Whether it performed any of those functions in January and February 2022 is not known. Its explicit terrorism and high-risk travellers focus may have limited its operational role with regard to acting as a fusion centre for intelligence on the “Freedom Convoy” protests. The degree to which the RCMP’s Ideologically Motivated Criminal Intelligence Team liaised with the NSIJOC is unknown.

Like CSIS, the RCMP may have been impacted in their overall efforts to use OSINT effectively by long-standing and unresolved issues around their collection and use of intelligence from social media monitoring. Like CSIS, it has faced public criticisms for its deployment of “spy” tactics. Very recently, these criticisms have come to focus on the use by the RCMP of commercial spyware to capture data from cell phones.

OSINT challenges for the RCMP date back to 2014, when the Civilian Review and Complaints Commission for the RCMP initiated two investigations into the RCMP’s handling of protests. One was a public interest investigation stemming from a complaint lodged by the BCCLA into the actions of the RCMP in investigating people involved in pipeline protests in British Columbia. The other was a Chair’s complaint and investigation into the RCMP’s action in managing protests over shale gas exploration by a company in New Brunswick that operated, in part, on land of the Elsipogtog First Nation. Both CRCC investigations came to essentially the same conclusions with regard to deficiencies in policy in the RCMP’s use of open-source intelligence.

Both investigations were slow moving; foot-dragging responses by the RCMP added further to the delay. The CRCC issued an interim report into the handling of the shale gas protests in 2019,
and received the RCMP’s response to its report in June 2020, in which the RCMP rejected some of its recommendations. The CRCC issued a final report on the shale gas protests in November 2020, six years after beginning its investigation. One of the recommendations rejected by the RCMP concerned the CRCC’s finding that the RCMP’s policy with regard to open-source intelligence collection was flawed and needed to be tightened up, especially with regard to the limits on collection of personal information from social media sites, the permitted use of such information, processes for verification, and limits on retention. The RCMP Commissioner provided to the CRCC a detailed defence of the RCMP’s use of open-source intelligence and its importance as an investigative tool for the handling of public protests, a need that extended beyond a criminal nexus. The CRCC was not satisfied by the Commissioner’s response. As the CRCC Chair put it, “The RCMP strongly rejected recommendations limiting collection and retention of open-source information. The Commission has serious concerns about the RCMP’s approach in such matters.” A similar impasse developed between the CRCC and the RCMP over the CRCC’s nearly identical recommendations in its final report on the use of open source intelligence in response to pipeline protests in B.C.

An internal audit was conducted by the RCMP into its policies for open-source intelligence while the CRCC investigations were still underway. The audit identified an RCMP practice that distinguished between three tiers of open source intelligence collection. Tier 1 was described as overt online activities which might involve such things as research, environmental scanning, inquiry and public engagement and was considered low risk. Tier 2 was labelled as passive online activities for intelligence and investigations that were designed to be “discreet”—that is there would be no direct engagement with any target of OSINT collection. Tier 3 was “covert” monitoring and was designed to hide and safeguard any RCMP OSINT collection. The audit released a final report in January 2021, based on a study of OSINT use between April 2018 and March 2019. The audit report reached a number of conclusions, including that internet related OSINT activities were not consistent or compliant with policy guidance and that a more robust governance framework was needed. Many employees, it found, were unaware of the existing policy—O.M. (Operational Manual) 26.5, “Using the Internet for Open Source Intelligence and Criminal Investigations.” The audit worried about risks to investigations “if users are not aware of the appropriate methods to capture, store and retain OSI [open source intelligence].” The risks identified included potential damage to court prosecutions, reputational risk, and the possibility of future imposed limitations on OSINT usage. The audit urged better training and information sharing.

The audit report also suggests that technological solutions for Tier 2 OSINT collection may have been incomplete, including the creation of a cloud-based solution, involving protection against attribution back to RCMP computers, and the use of smart phones for OSINT. As the audit noted, “Any enterprise-wide IT solutions for Tier 2 should consider the widespread use of mobile devices in addition to potential attribution risks, IM (Information Management) requirements, and privacy considerations.” In response the RCMP undertook to create a policy “hub” with centralized expertise on OSINT, which the audit had found was missing, and to establish an “Oversight Working Group” to help
develop a new policy suite and revise the existing O.M 26.5 document. All of this activity was meant to occur in 2020 and 2021, but the extent to which it was completed and applied is not known and work may have been delayed because of the pandemic.

Because of past high-profile criticisms and ongoing development work, the RCMP may not have been well placed to fully exploit OSINT as an important intelligence tool in response to the “Freedom Convoy.” Determining future OSINT needs for the RCMP would be an important part of any systematic review of the NSI system as a whole.

**The Canada Border Services Agency (CBSA)**

The Canada Border Services Agency was established in December 2003 as part of a wide-ranging overhaul of Canada’s security architecture and governance. The Agency is in the portfolio of the Department of Public Safety and Emergency Preparedness, created at the same time. The original establishment was based on an Order in Council; CBSA legislation followed in 2005. The CBSA Act does not list any specific national security, intelligence or law enforcement activities but provides the Agency with a high-level mandate that includes support for national security and public safety priorities.

The operations of the Canada Border Services Agency were profoundly impacted by the events surrounding illegal blockades at the border. These blockades went to the heart of CBSA’s mandate for border integrity at ports of entry and decision-making on admissibility of people and goods at the border. Four key ports of entry: at the Ambassador Bridge, Ontario; Coutts, Alberta; Emerson, Manitoba; and the Pacific Highway in British Columbia experienced multi-day closures because of the protests. Re-routing of border traffic was required.

Official border ‘Ports of Entry’ (POE) are secure, controlled areas not accessible to persons other than those crossing the border. It is a criminal offence under the Customs Act to hinder the work of a Border Security Officer (BSO), but it is important to note that CBSA does not have any jurisdiction or enforcement powers regarding protest measures taken to block access to ports of entry, such as the placing of concrete barriers or heavy machinery, beyond the limited, defined physical area of the POE. Such activities must be dealt with by police of jurisdiction. At two locations, CBSA officers had to lock down offices to prevent entry.

The Emergency Measures Regulations, proclaimed on February 15, 2022, gave CBSA a distinctive new power to prohibit entry of foreign nationals who were identified as seeking to participate in or facilitate a prohibited public assembly. CBSA confirmed a statement made by the Prime Minister that some foreign nationals were turned back at the border, though exact numbers were not provided.

While the operations of CBSA were affected by the border blockages, its response role was largely confined to managing alternative routes for cross-border traffic and, once the Emergencies Act was invoked, to identifying and prohibiting the entry of foreign nationals.
coming to Canada to engage in a prohibited public assembly. Whether CBSA produced a range of threat reporting during the “Freedom Convoy” border blockades is unknown.

The current wording of the Emergencies Act does not specifically provide for the securing of critical infrastructure, including critical infrastructure at the border. This is an element of the legislation that may require modernization, in the light of the experience of the protest activities in Ottawa and at border crossing points in early 2022. ¹⁹⁰ Legislative and/or regulatory change, including to the CSIS Act definition of threats to the security of Canada, may be necessary. Such changes may be considered in the light of the federal government’s current efforts to update its critical infrastructure strategy, which dates from 2009 and does not list border infrastructure among the ten identified critical infrastructure sectors. ¹⁹¹

**The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)**

FINTRAC, created in 2000, has been described by one commentator as a financial intelligence “clearing house.” ¹⁹² It operates at an intersection between financial institutions in Canada and law enforcement and national security partners. According to its statute, FINTRAC

*collects, analyses, assesses and discloses information in order to assist in the detection, prevention and deterrence of money laundering and of the financing of terrorist activities.*”¹⁹³

Under the act, financial institutions have a responsibility to report certain classes of suspicious transactions potentially related to money laundering and terrorism financing to FINTRAC. ¹⁹⁴ FINTRAC then takes the “Suspicious Transaction Reports” (STRs) provided to it, and assesses them on a ‘reasonable grounds to suspect’ standard. Based on assessment findings, FINTRAC can then proceed to make disclosure reports to law enforcement and other investigative bodies in the criminal and national security space. For threats to national security, FINTRAC may disclose to CSIS, an appropriate police force, CBSA, and the Department of National Defence. The designated information that FINTRAC may provide is laid out in the Act and involves a wide range of identifying information including the criminal record of a person involved in a suspicious transaction. Whether FINTRAC produced any disclosure reports related to financing of the “Freedom Convoy” has not been divulged.

FINTRAC’s intelligence collection mandate is mostly passive, in the sense that it receives reporting from financial institutions, but its Act allows it to augment that flow of intelligence with open source information and with data held by federal or provincial government partners, and by foreign states or international organizations, subject to established agreements.

One special bulletin published by FINTRAC in July 2021 studied the financial behaviour of IMVE threat actors. ¹⁹⁵ The bulletin was prompted by a series of new additions of IMVE organizations to the Criminal Code list of terrorist entities. The practice of listing terrorist entities was codified in the original anti-terrorism act of December 2001, but it wasn’t until 2019 that the first IMVE groups were listed. Currently the following IMVE entities are listed:
In its published study FINTRAC noted several features of financial behaviour by IMVE actors, distinguishing between lone actors, individuals funding IMVE networks, and organizers. Lone actors typically used personal funds and regular banking methods. Financial transactions were typically small and difficult to observe. Individuals funding IMVE networks with donations were observed to rely on payment processing companies and money services. Organizations used both personal and business accounts and while transactions tended to be small, they were also more observable given connections between IMVE threat actors and companies charged with various criminal offences.

The FINTRAC report urged financial institutions with reporting requirements to FINTRAC to pay heightened attention to indicators of IMVE related financing and added a IMVE indicator in its STR reporting form. The July 2021 report was a clear indication that FINTRAC was alert to the broad typology of IMVE financing. 197

On the available evidence, it seems unlikely that FINTRAC was able to add to the intelligence picture regarding the “Freedom Convoy.” This was partly a result of its specialized mandate and reporting structure; partly a reflection of its own findings on IMVE related financing. Some of the convoy organizers had started a “GoFundMe” fundraiser as early as January 14, but prior to the invocation of the Emergencies Act and the subsequent filing of new regulatory requirements, crowd-funding platforms and related financial service providers were not among the entities required to provide reports to FINTRAC.

The very specialised role played by FINTRAC raises questions about the need for a more broadly based economic intelligence capacity within the federal national security and intelligence system to provide reporting on economic threats to Canada’s national security.

Who’s On First?: The Government Operations Centre (GOC) and the Emergencies Preparedness Secretariat, PCO

The Government Operations Centre (GOC) was established in 2004 as an entity within the newly created department of Public Safety Canada. It was designed to play an important coordinating role regarding events of “national significance” during an emergency by sharing
information and intelligence with federal departments, the provinces and territories and other
countries, including the US.  

According to a current official description, the daily activities of the GOC including monitoring
the threat environment; “providing national-level awareness of situations that could evolve into
national emergencies;” preparing warning reports and integrated risk assessments;
coordinating whole-of-government response management; and providing support to senior
decisionmakers.

The occurrences it may scrutinise, among a wide range of natural hazards and human-induced
events, include “civil disturbance.”

In the context of the “Freedom Convoy” protest movement and its activities, publicly available
information about the actual role played by the GOC appears almost non-existent. A reference
in an internal email communication indicates that in late January the Centre was asked to “start
pulling together a ‘common picture’ report working with other Ops centres as well. A
subsequent tracking record for IRG meetings on February 12 and 13 indicated that the GOC was
being deployed as a “supporting department” in efforts to ensure that a holistic picture of the
available intelligence was at hand.

The indications are that the Government Operations Centre may have been sidelined during the
“Freedom Convoy,” protests for reasons that remain unclear. Its previous role in monitoring
protest demonstrations had proven controversial and this may have impacted on a decision to
avoid making the GOC a central clearing house for information and intelligence on the
“Freedom Convoy” protest.

Moreover, its role appears to have been subsumed by the work of a new secretariat in PCO that
was created to support the Minister of Emergency Preparedness, when that Ministerial
appointment was announced in the Fall of 2021. An internal email dated January 26 noted
that PCO EP (Emergencies Preparedness Secretariat) “will roll up GOC/ADM NS OPS debriefs
into a nightly common operating picture for Ministers of SSE (the Cabinet committee on Safety,
Security and Emergencies), Minister of IGA (Intergovernmental Affairs), and their respective
offices, as well as PMO.”

The Emergencies Preparedness Secretariat issued a series of daily unclassified “National
Operations” updates that referenced the “Freedom Convoy,” starting on January 25, 2022.
These were brief situational awareness reports that drew on open source intelligence and
information from law enforcement agencies. The daily ‘snapshots’ mostly lacked any strategic
assessment of the national security threat potentially posed by the protest movement, and to
that extent were of limited value as intelligence products. The updates drew on other reporting
by government agencies regarding IMVE threats, repeatedly stressing that:

“There is a concern that individuals with a range of views, some ideologically motivated with
violent extremist action, could exploit the convoy to promote action that pose a risk to the
public and officer safety. No substantiated threats or credible plans have been identified at this time.”

This reporting essentially replicated similar messages contained in ITAC and RCMP reports discussed earlier in my paper. The existence of multiple centres of reporting with overlapping messaging may ultimately have contributed to the decision taken just prior to the invocation of the Emergencies Act to task the PCO Intelligence Assessment Secretariat with the unusual mission of pulling together an “aggregate intelligence” picture.

A stable governance structure for unified threat reporting is an important element that appeared missing during much of the “Freedom Convoy” protests.

**On Public intelligence**

When the federal government announced the invocation of the Emergencies Act on February 14, 2022, the news was greeted by a degree of public shock and significant political division in Canada. Some Western provincial premiers argued that the use of the Emergencies Act was unnecessary. The Quebec premier stated that it should not be utilised in his province. The Conservative party decried it as a form of wedge politics. The interim leader of the party argued that it was an “irresponsible escalation.”

The leader of the New Democratic Party, Jagmeet Singh, told the House of Commons that the use of the Act was a product of a failure of leadership, and that governments “did not take the threat of this convoy seriously.” He characterised the goal of the protest movement as to “overthrow a democratically elected government.” Mr. Singh indicated that his party would support the use of the Emergencies Act but added, “We will be watching. And we will withdraw our support if these powers are misused.”

The Canadian Civil Liberties Association came out as opposed to the measure because it felt the legal thresholds in the Act had not been met. The Toronto Star published an editorial that stated that “the protests and blockades could and should have been resolved by good intelligence, smart planning, and effective coordination among police forces.” Experts were divided.

The nature of the response was in part predicated on the fact that the Emergencies Act had never before been used, since its creation as a successor to the War Measures Act in 1988. But the circumstances around the invocation of the Emergencies Act, late in the manifestation of the “Freedom Convoy” protest, and the attendant political discord, raises an important question about the public use of intelligence by a government in power. The question is: should the federal government have made public, in some form, its intelligence on the threat posed by the “Freedom Convoy,” prior to the invocation of the Emergencies Act?

This is a controversial issue, but not outlandish. Intelligence no longer resides permanently behind a secret curtain, never to be revealed. It can have a role to play in public warning, objective truth-telling, and in response to disinformation. We have only to consider the remarkable ways in which intelligence has been used in public by key Western allies (and to a
small degree by Canada) in responding to the Russian invasion of Ukraine on February 24. This effort began even before the Russian attack. US and UK intelligence assessments pointing to a Russian premeditated assault on Ukraine were declassified and used in briefings to the media and in talks with foreign allies. In January the British Foreign Office issued a statement that Putin wanted to install a pro-Moscow regime in Ukraine. It said it was making the intelligence assessment findings public because of the “exceptional circumstances.” One week before the Russian attack the UK Ministry of Defence, on its twitter feed, posted an intelligence update which stated that “Russia retains a significant military presence that can conduct an invasion without further warning.” The tweet was accompanied by a map showing the likely invasion routes to be used by the Russian armed forces (all of which proved accurate one week later). Since the invasion began, the UK MOD has issued a near daily social media intelligence update on highlights of the Ukraine war.

The then chief of UK Defence intelligence, Lt. Gen. Sir Jim Hockenhull, gave an interview to the BBC in which he explained the unusual decision to use intelligence in the public domain, arguing that the decision wasn’t easy but that he felt it necessary—“to get the truth out before the lies come.” Another UK intelligence chief, the head of the Government Communications Headquarters, Britain’s signals intelligence agency, told an Australian audience that: 

*It is already a remarkable feature of this conflict [the war in Ukraine] just how much intelligence has been so quickly declassified to get ahead of Putin’s actions. From the warnings of the war. To the intelligence on false flag operations designed to provide a fake premise to the invasion. And more recently, to the Russian plans to falsely claim Ukrainian use of banned chemical weapons. On this and many other subjects, deeply secret intelligence is being released to make sure the truth is heard. At this pace and scale, it is really unprecedented.*

Sir Jeremy Fleming added, “In my view, intelligence is only worth collecting if we use it, so I unreservedly welcome this development.”

But can decisions to release intelligence in public to counter a foreign state adversary with a formidable apparatus of disinformation, no restraints on its use, and control of its domestic information space, engaged in waging an illegal war that threatens the stability of the global order, really be analogous to the situation that faced the federal government in January and February 2022? Put another way, could a government legitimately use intelligence in the domestic public domain to try to inform public opinion, counter disinformation, and possibly deter elements of a protest movement or reduce the threat it posed?

Clearly, the circumstances in which the federal government might consider releasing into the public domain current intelligence about domestic and non-state threats to national security in a time of emergency must be carefully weighed. Such unprecedented (for Canada) use of intelligence would have to factor in a whole host of considerations. At least eight arise, and others may be thought of.
The first would be simply to underline that such use of public intelligence would have to be considered on a case-by-case basis and severely restricted to protest demonstrations that posed clear threats to national security and engaged in significant disinformation. A second would be whether the government possessed intelligence about a national security threat that it had full confidence in and was prepared to defend in public. A third would be whether such intelligence could be safely declassified without threatening sources and methods of intelligence or interfering with ongoing criminal investigations. A fourth would be whether the release of intelligence could be managed in such a way that it was not seen as propaganda or as designed to advance the political interests of the government in power. Such release would have to come from a “trusted” official source. A fifth, very significant consideration, would be whether the use of intelligence in the public domain would be seen as a Charter violation, threatening free speech and assembly rights. A sixth would be possible impacts on privacy rights of any named individuals, especially leaders of a protest movement. A seventh calculation would be whether such intrusion by the government into domestic reporting would seriously impact and distort media coverage. A final calculation would be about ‘blowback.’

Would such public use of intelligence only exacerbate tensions and divisions around a protest movement?

These are all high hurdles, on top of the precedent-setting nature of any such use. Every single consideration would have to be carefully weighed.

To even contemplate such an action two things would have to be determined to properly limit the scope. One is that any exercise of the use of intelligence in public would be strictly fact-based. This could not be undertaken as an “information operation” in the military sense. The other would be that the primary rationale would be to target disinformation—to “get ahead of the lies.” Such restrictions make the idea of the public use of intelligence less outlandish and more in keeping with the kind of public information campaign that a police force might routinely use (and in the case of the OPS, did use).

What would be the benefits? Any such use of intelligence would be heavily reliant on OSINT, and would reinforce the importance of OSINT among intelligence collection sources. The idea that intelligence might be used in the public domain might introduce additional rigour into the intelligence process, to ensure accuracy and meet contestability standards. The use of public intelligence would be a clear signal of its importance to decision-making at the senior-most levels. Public knowledge and debate could be enhanced. A protest movement that posed a threat to national security could be undermined.

This weighing action is purely hypothetical in the context of the invocation of the Emergencies Act. There is no indication that releasing intelligence in public was ever considered, prior to February 14 or in the aftermath of the proclamation of a Public Order Emergency.

This brief examination of the potential uses of public intelligence is stimulated by the confusion and discord that surrounded the invocation of the Emergencies Act. Its justification is forward-looking. The more that a variety of national security threats, some open, some more hidden,
threaten our democracy, the more necessary it might become to bring intelligence into the public domain, with the proper safeguards and decision-making process.

**On Review and Accountability:**

In a public address hosted by the Centre for International Governance Innovation in February 2021, CSIS Director David Vigneault remarked: “Keeping Canada safe requires a national security-literate population. By this I mean a citizenry that understands the key dilemmas Canada faces, and recognizes the need to adapt and respond in a thoughtful, meaningful, and timely way.”

One of the principal means by which the goal of a national security literate population can be advanced is through the work and reporting of independent review bodies.

The Public Order Emergencies Commission is a powerful review and accountability tool, so designed by the 1988 legislation. It takes its place alongside the key elements of Canada’s new review system—the National Security and Intelligence Committee of Parliamentarians, the National Security and Intelligence Review Agency, and the Intelligence Commissioner (properly an oversight body)—in offering Canadians answers to important questions about the use of government powers. Like the review system, the Commission will have to find its own balance between compliance and efficacy issues, between lawfulness and performance. Like the review system, the Commission will make recommendations for improvements.

Both the Commission and the review system share a common question as Canada faces a new world of threats—that question is: what is the role of intelligence in protecting democracy? This is not a question Canadians are used to asking in recent years. As troubling aspects of the “Freedom Convoy” demonstrated, a national security environment beset by disinformation and misinformation, by conspiracy theories, by foreign interference, by concerns about IMVE threats, by virulent distrust of government, by attacks on critical infrastructure, by societal trauma and division caused by the impacts of two years of an unprecedented public health crisis, all require that we seek answers and make necessary adjustments to our thinking about intelligence, with a more mature leaning away from concerns about intelligence practices being a threat to democracy itself, and towards a notion that intelligence can be a safeguard for democracy, if appropriately used.

Was the intelligence system ready and able to be a safeguard in response to the events of the “Freedom Convoy” protest? Canadians deserve a full answer to that question, not least to prepare for the future.

**Conclusion: Findings and Issues for Future Study**
Understanding the role played by intelligence reporting on potential threats posed by the “Freedom Convoy” protests should be central to the work of the Public Order Emergencies Commission and to future thinking about Canada’s national security needs. The Commission’s mandate directs it to “examine and report on the circumstances that led to the declaration of a public order emergency...” There is no more important ‘circumstance’ than the performance of the intelligence function. Intelligence should have provided the basis for informed decision-making in response to the “Freedom Convoy” at all levels from local law enforcement to the Cabinet table.

The question must be asked—was there an intelligence failure with regard to understanding the intentions, capabilities, and operations of the “Freedom Convoy” protest?

Intelligence failure occurs when there is a failure of early warning, allowing for a surprise threat to take shape and have impact, or when there is a failure to assess a threat situation accurately, leading to a failure in response. As the expansive literature on intelligence failure records, deficiencies can occur at every stage of the intelligence cycle, including collection, analysis and reporting—they can occur as a result of cascading failures across the entire cycle. Policing failures in confronting a protest are inseparable from intelligence failures. One feeds the other.

Any answer to the intelligence failure question must be nuanced and must be predicated on an assumption that there existed a realistic possibility of providing early warning and accurate, forward-looking situational assessments. If the “Freedom Convoy” protest simply evolved and mutated, at speed, beyond the control of its organizers and elements within its midst, and according to no set plan, then that realistic possibility does not exist. An intelligence system cannot be expected to predict the unpredictable or know the unknowable. It is not a crystal ball.

Any findings regarding intelligence failure based solely on the extant public record at the time of writing are liable to be partial and possibly wrong. But there are troubling features to the performance of the national security and intelligence system in response to the “Freedom Convoy.”

The most striking is that there was no demonstrated ability to assess the capabilities and intentions that animated the “Freedom Convoy.” Intelligence reporting simply left decision-makers guessing.

Some of the operations of the “Freedom Convoy”, including its online fund-raising successes, its tactical use of heavy equipment and “weaponizing” of trucks, its border blockades, the presence of children among the protesters, and the ways in which its messages metastasized across Canada and beyond, took the national security and intelligence system by surprise and forced it into a reactive mode.

There were multiple streams of threat reporting and efforts to pull together an integrated intelligence picture, as indicated by the IRG records, came very late in the day.
OSINT, as an intelligence methodology, underperformed for reasons that deserve further scrutiny. It could and should have been a rich intelligence resource, given the reliance of the Freedom Convoy leadership and followers on social media messaging. But OSINT requires resources, technological capacity, and analytical skill sets that may have been unavailable. It has to be valued by the NSI system and by decision-makers. Concerns about the limitations of authorities for the national security and intelligence system may also have been a hindrance.

The national security and intelligence system maintained a narrow focus in its threat reporting on concerns about IMVE. While in keeping with lawful mandates, the ways in which this narrow focus was operationalized significantly reduced the value of intelligence.

Threat reporting in general missed the significance of critical infrastructure vulnerabilities, especially at the border, and the prospect of significant supply chain disruptions.

Collective, Cabinet-level governance, as represented by the IRG, came into play too late in the crisis and encouraged emergency thinking.

Sub-cabinet level operations in the NSI committee system may have had a better handle on the threats posed by the “Freedom Convoy,” but until the records of the ADM NSOps committee can be investigated, this is speculation. All that can be said was that the early intent was there as expressed by the desire, as the Assistant Secretary to the Cabinet put it, to have “structure and governance on this issue…”

The idea of using public intelligence as a way to inform the public and prepare the ground for responses by the federal government was never contemplated. Such action would have been unprecedented. It may also have been helpful.

The threat reporting paid little attention to any subversive threat opposed by the “Freedom Convoy”.

If these are indicators of failure, they must be weighed against elements of success, to provide a balanced picture. CSIS, ITAC, the RCMP, and the Emergency Preparedness Secretariat all appear to have been cautious in their assessment of the nature of the IMVE threat posed by the “Freedom Convoy,” drawing attention to the possibility of incitement to violence through extremist rhetoric, particularly online, and to the possibility of lone actor attacks. The intelligence system was paying attention to online extremist rhetoric disseminated by elements of the “Freedom Convoy” protest.

It has to be deemed a success that the “Freedom Convoy” was never painted with a broad brush as posing a terrorist threat. Rather the depiction was of a protest movement that became unlawful and contained the possible seeds of violence. The notion that the “Freedom Convoy” might generate any kind of coordinated or dangerous terrorist attack on the parliamentary precinct was dismissed.
In short, the NSI system avoided creating an exaggerated terrorist threat picture, for which they deserve some credit. The NSI system proved less capable of generating a more holistic understanding of anti-authority/anti-democratic, subversive, economic, and foreign interference dimensions of the “Freedom Convoy” threat.

The overt and narrow focus of the NSI system on IMVE threats stemmed from mandate authority limitations of such organizations as CSIS, ITAC and the RCMP. This raises the question of the overall capacity of the Canadian national security and intelligence system to pivot to potential threats posed to our democracy. In particular it may require new thinking about a stand-alone open source intelligence centre, decoupled from the CSIS Act and with its own statutory or regulatory authority, supported crucially by transparency about its mission, collection capabilities and objectives. It would be necessary to provide such a centre with sufficient “social licence,” as it would be bound to be met by concerns about mass surveillance and privacy intrusions. The record of previous public criticisms of alleged spying on protest movements by CSIS, the RCMP, and the Government Operations Centre documented in this report underscores this need. There would need to be a clear public review and accountability regime for such a centre.

The creation of a stand-alone OSINT centre would reflect lessons from the “Freedom Convoy” experience about both the importance of this intelligence methodology and the challenges involved in ensuring its effectiveness, including governance challenges around integration. Multiple streams of OSINT-based threat reporting, as witnessed during the protest movement, are not efficacious and may only serve to lessen the impact and appreciation of such an intelligence source. They may also create an “echo chamber” effect in which assessments become duplicative, especially if there is no built-in challenge function.

Given the role played by the NSIA, as demonstrated during the events of the “Freedom Convoy,” an open source centre would best placed in PCO, reporting to her.

Developing such an OSINT centre would be one way to ensure that the Canadian national security and intelligence system has the capabilities, resources, governance structures and authorities needed to respond appropriately to future, broad-based threats to democracy. But it will only be one way and the experience of NSI system responses to the “Freedom Convoy” reinforces the need for a comprehensive examination of the capabilities and authorities of the NSI system as a whole. No such comprehensive examination has ever been undertaken in the history of the Canadian NSI system.

Intelligence failures always matter. In the context of the invocation of the Emergencies Act a putative intelligence failure may have deprived the federal government of decision time, narrowed opportunities to consider alternative policies, and reduced flexibility. It may have driven reactive decision-making and contributed to paving the way for a “last resort” measure. These are high consequences.
The centrality of the CSIS Act and its definition of threats to the security of Canada was evident during the reporting on the “Freedom Convoy,” notably in the emphasis given to IMVE concerns. The CSIS Act definition of threats to the security of Canada and its operational mandate at section 12 are thirty-eight years old, a product of an earlier and searing historical experience for Canada, of a vastly different threat environment, and reflective of an age with very different intelligence methodologies. The CSIS Act needs a thorough-going review to ensure that it provides the Service with a modern, fit mandate, while maintaining adherence to Canadian laws and democratic norms.

Alongside questions of intelligence failure and possible fixes, there is a related issue: in what ways does the language of the 1988 Emergencies Act need to be modernized to ensure that it remains relevant in future, as we confront threat environments that could not have been imagined thirty-four years ago? In particular, do threats to national security need to be redefined in the Act and should protection of critical infrastructure, economic security, and harms to international relations, be incorporated in the statute for a Public Order Emergency? 226

As the CSIS Director stated in a public speech following the “Freedom Convoy” protests, “the fight for democracy is one we cannot afford to lose.”227

The national security and intelligence system must be equipped for that fight, in ways that the Canadian public has a chance to debate, understand and accept. The available evidence and tentative judgement is that the NSI system was not ready and fully equipped when the “Freedom Convoy” descended on Ottawa and critical infrastructure at the border. If there is one statement that bears witness to this lack of readiness and absence of intelligence foresight, it was provided by RCMP Commissioner Lucki. Commissioner Lucki testified on May 10 that: “I think, when people came to Ottawa, people honestly thought that they were going to do their thing on the weekend and then were going to leave after the first day that Parliament resumes”. “Obviously,” she said, “that did not happen.”228

ENDNOTES

4 National Security and Intelligence Committee of Parliamentarians (NSICOP), Annual Report 2018, published in redacted form April 2019, noted “Canadians do not appear to have a strong understanding of the individual mandates or activities of the organizations of the security and intelligence community, how they work together, or
5 Allegations of “false flag” operations by protesters were noted in RCMP threat reporting, see IMCIT Special Threat Advisory, Update 5, February 3, 2022, ATIP release package A-2021-00438. Copy in the possession of the author. For one such narrative by a self-proclaimed “intelligence office” for the “Freedom Convoy,” see an interview with Tom Quiggin, Saskatchewan Today, August 5, 2022, https://www.sasktoday.ca/south/local-news/protests-at-police-stations-could-turn-violent-military-expert-5663148
8 I am very grateful to Canadian journalist who willingly provided me with copies of records released to them through the Access to Information Act
13 Erik J. Dahl, Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond (Georgetown University Press, 2013)
15 David Omand, Securing the State, (NY: Columbia University Press, 2010), p. 9
19 Sir Mark Rowley, “Open Source Intelligence”  
22 David Omand, Jamie Bartlett and Carl Miller, “Introducing social media intelligence (SOCMINT),” in Secret Intelligence: A Reader, pp. 77-94
23 Gibson, pp. 100-101
27 ibid
31 Canadian Anti-Hate Network, January 27, 2022, “The ‘Freedom Convoy’ is nothing but a vehicle for the far right,” https://www.anticlave.ca/the_freedom_convoy_is_nothing_but_a_vehicle_for_the_far_right
34 Wesley Wark, “No More polls: Canadians want more information about spying,” The Hill Times, January 26, 2022, https://www.hilltimes.com/2022/01/26/no-more-polls-canadians-want-more-information-about-spying/339904; National Security and Intelligence Committee of Parliamentarians (NSICOP), Annual Report 2018, published in redacted form April 2019, noted “Canadians do not appear to have a strong understanding of the individual mandates or activities of the organizations of the security and intelligence community, how they work together, or the role of review bodies,” p. 23.
36 ibid
38 Cabinet committees, https://pm.gc.ca/en/cabinet-committee-mandate-and-membership#security
39 ibid
40 There are indications in the available record that the Safety, Security and Emergencies Committee was also engaged. See Mike MacDonald email to NSIA and others, January 26, 2022, which notes that PCO EP (Emergency Preparedness Secretariat) would be presenting reporting “for Ministers of SSE.” ATIP release package, A-2021-00438. Copy in the possession of the author.
41 A copy of the PCO organization chart is available at: https://www.canada.ca/en/privy-council/corporate/organizational-structure.html
44 For a full discussion, see the seminal text by Craig Forcese and Leah West, National Security Law, 2nd edition (Irwin Law, 2020); See also Craig Forcese and Kent Roach, False Security: The Radicalization of Canadian Anti-Terrorism (Irwin Law, 2015)
51 In testimony before the Security and Intelligence Review Committee (SIRC) in August 2015, the CSIS Director General for the BC region noted that, to his knowledge, the Service had not conducted a subversion investigation for the last 20-25 years. SIRC report, file 1500-481, 2017, published by the British Columbia Civil Liberties Association, in its “Protest Papers” series, Vol. 1, https://bccla.org/secret-spy-hearings/#protest-papers
59 ibid
60 Copies of the redacted IRG meeting records, released by the Federal Court, in the possession of the author. Cited as IRG Minutes.
61 IRG Minutes, February 10, 2022
62 ibid
IRG Minutes, February 12, 2022. Select Deputy Ministers had met to discuss the Freedom Convoy as early as January 25, according to an email from Mike MacDonald to the NSIA, January 25, 2022, ATIP release package A-2021-00438. Copy in the possession of the author.

Minutes of The Cabinet, February 13, 2022, 8:30 p.m.


Ashley Burke, CBC News, “Trudeau’s intelligence adviser backs use of Emergencies Act to clear Ottawa convoy protest,” March 10, 2022, https://www.cbc.ca/news/Politics/jody-thomas-overthrow-federal-government-1.6379881 No transcript of Ms. Thomas’s address has been made available. Ms. Thomas’ remarks came in response to a question from the audience to a panel moderated by Richard Fadden, a former NSIA. A live-stream clip of her remarks (4:12 minutes) is available online at: https://www.ctvnews.ca/politics/convoy-organizers-had-extreme-aims-says-pm-s-national-security-adviser-1.5814097

Email Mike MacDonald to the NSIA/PCO officials, January 24, 2022. ATIP release package A-2021-00438. Copy in the possession of the author.

Email Mike MacDonald to NSIA/PCO officials, January 26, 2022

Email Mike MacDonald to NSIA/PCO officials, February 2, 2022

No IAS reporting on the “Freedom Convoy” has been released into the public domain


Capabilities assessments are a common feature of military intelligence work, often referred to as “order of battle” intelligence.

NSIA, Ms. Thomas remarks at a conference in Ottawa, March 10, 2022. :
https://www.ctvnews.ca/politics/convoy-organizers-had-extreme-aims-says-pm-s-national-security-adviser-1.5814097

In opening remarks to the IRG on February 12, the Prime Minister stated that “he has been speaking with a number of international partners and they are all expressing concern about Canada and our ability to handle it.”


Testimony of CSIS witnesses, recorded in SIRC Report, BCCLA Complaint, file 1500, ibid


ibid, p. 24

ibid, p. 25


NSIRA Review 2019-04


ibid, paras 107-08


115 ibid
130 Ibid (Minister Blair, p. 31 at 21:21)
131 Ibid (Minister Blair, p. 32 at 21:27)
133 Ibid., p. 11
134 Ibid., p. 18
135 This passage is based on personal and confidential knowledge, some gained while serving on the Prime Minister’s Advisory Council on National Security between 2005 and 2009, and on discussions with early leaders of ITAC.
138 For a brief description of ITAC’s current role see Stephanie Carvin, Stand on Guard: Reassessing Threats to Canada’s National Security (University of Toronto Press, 2021), p.285; Carvin provides a more extended analysis of ITAC in a chapter in Stephanie Carvin, Thomas Juneau and Craig Forcese, eds., Top Secret Canada: Understanding the Canadian Intelligence and National Security Community (University of Toronto Press, 2020), chapter 5.
ITAC Report, “Request for Information, “Violent Extremist Threats to Four Specific Ministers,” January 31, 2022. Justin Ling, “Canada was warned before protests that violent extremists infiltrated convoy,” The Guardian, February 17, 2022, https://www.theguardian.com/world/2022/feb/17/ottawa-protests-anti-terror-agency-warned-violent-extremists; this report led retired CSIS terrorism analyst, Phil Gurksi, a frequent commentator, to proclaim that CSIS was properly on the job, despite admitting that he had no access to any of the intelligence reporting, “Canada’s spies were right about the ‘Freedom Convoy,” The Ottawa Citizen, February 21, 2022, https://ottawacitizen.com/opinion/gurski-canadas-spies-were-right-about-the-freedom-convoy. This Op Ed piece made its way into ITAC files.


ITAC Threat Highlight, “Canada: Extremists may attempt to seize the opportunity of public protest,” TH 22/08-A, January 27, 2022, ITAC ATIP package

4Chan is an anonymous chat forum. It is unsupervised and uncensored, and features dedicated topic threads. Posts are deleted after a period of time (usually after a few days).


Ibid

ITAC Threat Highlight, “Canada: IMVE threats in the context of public protest,” TH 22/10-E, February 3, 2022, ITAC ATIP package

ITAC, Threat Highlight, “Canada: IMVE threats in the midst of anti-vaccine protests in the NCR and across the country,” TH-Generic, February 7, 2022, ITAC ATIP package

Ibid. The threat assessment noted the involvement of conspiracy theorist Romana Didulo (misspelled Roman Didulo)


ITAC Threat Highlight, “Canada: Update: Threat to uniformed personnel unchanged despite increase in online violent rhetoric,” TH 22/12-E, February 10, 2022, ITAC ATIP package

ITAC Threat Highlight, “Canada: Update: Threat to uniformed personnel unchanged despite increase in online violent rhetoric,” TH 22/12-Corrected, February 11, 2022, ITAC ATIP package


ITAC Threat Highlight, “Threats to Canadian political figures and government locations in the context of protests and emergency response mechanisms,” TH 22/13-E, February 24, 2022. ITAC ATIP package

ITAC Threat Highlight, “Threats to Canadian political figures and government locations in the context of protests and emergency response mechanisms,” TH 22/13-E, February 24, 2022. ITAC ATIP package

ITAC, Threat Highlight, “Canada: IMVE threats in the midst of anti-vaccine protests in the NCR and across the country,” TH-Generic, February 7, 2022, ITAC ATIP package

ITAC Update 1: “Ideological Extremism (Anti-Authoritarianism and Anti-Government)” February 17, 2022, ITAC ATIP Package


A suggestion made in 2004 to this effect was rejected by a senior official at PCO (Private knowledge).


CSIS-RCMP Framework for Cooperation, One Vision 2.0, https://secretlaw.omeka.net/items/show/21

NSIA Talking Points, DM Weekly, February 9, 2022, ATIP release package A-2021-00438. Copy in the possession of the author


166 ibid.

167 IMCIT Special Threat Advisory, Update 1, January 26, 2022.

168 Ibid.


170 IMCIT Special Threat Advisory, Update 4, January 31, 2022.

171 IMCIT Special Threat Advisory, Update 5, February 3, 2022.

172 IMCIT Special Threat Advisory, Update 6, February 10, 2022.


174 IMCIT Special Threat Advisory, Update 6, February 10, 2022.


182 Executive Summary, Ibid


185 “Conclusion,” Ibid.


187 Ibid.
The federal government recently concluded a round of public consultations in the summer of 2022 on modernizing the critical infrastructure strategy, see https://www.letstalkcriticalinfrastructure.ca


FINTRAC, Strategic Intelligence, “FINTRAC, law enforcement and intelligence partners: Sharing intelligence, making the links,” https://fintrac-canada.gc.ca/intel/general/1-eng


The description provided in a 2009 Auditor General’s report on emergency management indicated that the GOC “keeps other departments informed of the status of events on a real-time basis and alerts them if the events escalate into a more serious situation.” It was, by that time, producing regular situation reports and operating on a 24/7 basis. Overall, the Auditor General’s 2009 report was critical of Public Safety for failing to exercise leadership to coordinate emergency management activities, but developments with the GOC were seen as a bright spot.


Email message, Mike MacDonald to NSIA and other recipients, January 25, 2022, ATIP release package, A-2021-00438, copy in the possession of the author.

Ibid, p. 14; Incident Response Group meeting record, February 12, 2022, p. 15


Email Mike MacDonald to NSIA, January 26, 2022, ATIP release package, A-2021-00438. Copy in the possession of the author.


Ibid
210 ibid
211 https://www.thestar.com/opinion/editorials/2022/02/14/invoking-the-emergencies-act-is-a-shocking-admission-of-failure.html
212 As an example of the extensive media coverage regarding the February 14 announcement, see https://www.cbc.ca/news/politics/trudeau-premiers-cabinet-1.6350734
215 UK Ministry of Defence, February 17, 2022, “Intelligence Update,” https://mobile.twitter.com/DefenceHQ/status/1494315294382297091?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembedded%7Ctwterm%5E1494325839462236173%7Ctwgr%5E%7Ct wc@n%5Es3_&ref_url=
216 UK MOD Intelligence Update for August 31, 2022, https://twitter.com/DefenceHQ/status/1564843163839258624
219 ibid
221 Issues around the uses of intelligence and lawfulness were a prominent part of the work of the McDonald Commission, in the late 1970s and early 1980s, which helped usher in the Canadian Security Intelligence Service. For an overview, see Reg Whitaker, Gregory S. Kealey and Andrew Parnaby, Secret Service: Political Policing in Canada from the Fenians to Fortress America (University of Toronto Press, 2012)
224 Email Mike MacDonald to NSIA and PCO officials, January 24, 2002. ATIP release package A 0392. Copy in the possession of the author.