



Summary Report

Author: Stephanie Carvin, Associate Professor, Norman Paterson School of International Affairs, Carleton University

Panel Theme: Canada's National Security Apparatus

Do Canada's intelligence agencies have the legal authorities, technical capabilities and resources necessary to detect, collect, and analyze information regarding foreign interference, especially in the online environment.

Developments post-Bill C-70

By and large, Canada now has the correct authorities to investigate foreign interference activities that impact “political or governmental process in Canada”, with two possible exceptions.

Media and Foreign Interference Transparency: First, there may be a gap illustrated by the recent allegations made in the United States about Russian-entities funding media outlets to push far-right narratives.¹ As counter-threat financing specialists have noted, individuals involved in such an enterprise in Canada would not be required to register as foreign principals under the *Foreign Influence transparency and Accountability Act* because “this component of the *Act* only applies to individuals and entities engaged in influencing political and governmental processes.”² In other words, there is nothing in the current legislation that requires the disclosure of payment by foreign actors for the creation of content included in the final draft of the bill.

The question here is whether it is desirable to have a foreign interference transparency registry scrutinize sectors that are not “political” but may have political influence, like the media. This issue raises challenging questions about media freedom, which is fundamental to our democracy which should be a part of a much broader discussion and consultation around these issues before any such changes are made.

¹ U.S. Department of Justice, “Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere”, 4 September 2024. <https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence>

² Jessica Davis, “Networks of Deception: Russian propaganda, foreign interference, sanctions evasion and the Canadian connection”, *Insight Monitor*, 17 September 2024. <https://newsletter.insightthreatintel.com/p/networks-of-deception-russian-propaganda>



Intelligence to Evidence: The longstanding “intelligence to evidence” problem was not addressed in Bill C-70. This is a complex issue, and there is not the space to discuss fully here. Moreover, other, more qualified individuals have discussed it thoroughly elsewhere.³ However, it is important to note that the “intelligence to evidence” problem continues to be a serious gap in our ability to prosecute national security offences. Ultimately, capacity to pursue foreign interference investigations will come to little if Canada remains unable to prosecute these offences in court.

However, I wish to stress that other than these two issues, most of the challenges presently experienced by the national security and intelligence community relate to problems of capacity, rather than gaps in our legal framework. Indeed, I am concerned that with Bill C70 the government has fixed laws for deficient institutions. Without major reform of how national security agencies, especially the RCMP, operate and allocate their resources, it is unlikely that there will be a substantial improvement in how foreign interference is investigated, prosecuted and countered in Canada.

Recruitment, Retention and Training

Recruitment: That national security and intelligence agencies are struggling with recruitment and retention has been well established in both news media and public reports.⁴ In interviews conducted with members of the national security and intelligence community in 2018-2019 revealed that they had serious concerns about their ability to recruit, with one individual naming it as their organization’s “number one corporate risk”.⁵ It is likely that the situation has gotten worse in the ensuing years. Budget cuts, a paralyzed clearance process that can take up to two years to complete, and retention issues are seriously hampering the ability for the community to staff itself to fulfill its mandate. Replacing individuals who are retiring or leaving is difficult, leading to a loss of expertise when it is needed most, and burn out among staff who are asked to cover several positions for extended periods of time.

Workplace culture: Moreover, key agencies like the RCMP and CSIS continue to face criticism over problems related to human resources management, workplace culture toxicity, sexism, harassment and racism. This includes 6 reports on the Royal Canadian Mounted Police (RCMP)⁶ and multiple lawsuits brought against CSIS resulting in several

³ Craig Forcese and Leah West, *National Security Law*, 2nd Edition, Toronto: Irwin Law, 2021. pp. 660-666; Craig Forcese, “Threading the Needle: Structural Reform & Canada’s Intelligence-to-Evidence Dilemma”, *Manitoba Law Journal*, Vol. 42, No. 4, 2019. pp. 131-187.

⁴ Catherine Tunney, “Recruitment, retention ‘issues of concern’ for CSIS: internal docs”, CBC News, 14 August 2019. <https://www.cbc.ca/news/politics/csis-recruitment-retention-1.5245126>.

⁵ Thomas Juneau and Stephanie Carvin, *Intelligence Analysis and Policy Making: The Canadian Experience*, Stanford: Stanford University Press, 2021. p. 51.

⁶ This includes The Standing Senate Committee on National Security and Defence: *Conduct Becoming:*



settlements.⁷ There can be little doubt that such an environment only exacerbates problems related to recruitment and retention. It is also likely that toxicity in the workplace, beyond impeding safety for employees, will inhibit the kind of teamwork necessary to engage in complex investigations necessary for countering foreign interference. While steps have been taken to address workplace safety, ongoing and well-resourced efforts to counter this problem will be needed for the foreseeable future.

Contract policing: Beyond this, the RCMP finds itself in a position where the federal policing branch of the organization is consistently losing staff to fulfill provincial contract policing positions.⁸ Unfortunately, there are several barriers preventing the federal policing side from easily replacing and retaining these members, beyond the factors identified above. First, new recruits at Depot (the primary training facility) are trained in general duty policing and lack experience and knowledge to work national security investigations. Second, there are fewer promotional opportunities on the federal policing side, which means that officers with national security investigation experience transfer back to provincial policing after a few years, leading to fewer experienced staff to investigate.⁹ While it is beyond the scope of this brief to provide a full answer to the problem of contract policing, the government should take heed of the many studies that have drawn attention to this problem.¹⁰ It should find ways to better support the federal policing mandate (possibly by creating two separate forces which focus either on contract or federal policing) or consider abandoning the provincial policing mandate entirely.

Training and the generalist model: However, even when there are adequate personnel, questions have been raised about the sufficiency of the training that RCMP officers receive. The 2023 *Special Report* by NSICOP found that “Federal Policing has struggled to source all the skills, education and experience required to conduct increasingly complex and specialized investigations in the modern criminal threat environment.”¹¹

In part, this highlights challenges around the “generalist” model used by CSIS and the RCMP when it comes to training. In both cases, these agencies provide a basic skill set to their

Why the Royal Canadian Mounted Police must Transform its Culture (2013); Civilian Review and Complaints Commission for the RCMP, *Report into Workplace Harassment in the RCMP* (2017); Sheila Fraser, *Review of four cases of civil litigation against the RCMP on Workplace Harassment* (2017); The Honourable Michel Bastarache, *Broken Dreams, Broken Lives: The Devastating Effects of Sexual Harassment On Women in the RCMP* (2020); The House of Commons Standing Committee on Public Safety and National Security: *Systemic Racism in Policing in Canada* (2021); *Mass Casualty Commission report on the April 2020 mass casualty in Nova Scotia* (2023); NSICOP, *Special Report on the Federal Policing Mandate of the Royal Canadian Mounted Police* (2023).

⁷ Jim Bronskill, “Canada’s spy service to hire human rights specialist amid harassment claims”, *Global News*, 14 December 2023. <https://globalnews.ca/news/10169636/csis-human-rights-reviewer/>

⁸ NSICOP, *Special Report*, pp. 54-57.

⁹ NSICOP, *Special Report*, p. 57.

¹⁰ See, especially, NSICOP, *Special Report*.

¹¹ NSICOP, *Special Report*, p. 58.



officers, but no specialized training before they undertake complex investigations related to money laundering, sanctions evasion, cyber security or foreign interference. Instead, staff are expected to learn as they go on the job. Moreover, individuals can show up to work one day and find out that they are being pulled from a counter-terrorism file to a counter-espionage file and vice versa. The individuals go where the needs are – that is the nature of our system. But is a difference with some of our Five Eyes partners where individuals develop subject matter expertise over several years, if not decades.

This approach to training and learning on the job represents a 20th Century approach to national security that is no longer fit for 21st century level threats. Without providing specialized knowledge and training, individuals tasked with investigating foreign interference may lack expertise, leading to mistakes when it comes to gathering intelligence or evidence, leading to faulty investigations or failed prosecutions. For example, the RCMP's failure to properly gather digital evidence on a computer resulted in an acquittal of an individual in a case of sanctions violation – one of the few times Canadian authorities have tried to prosecute such a case.¹² This case highlights the need for the national security and intelligence community to invest in the specialization of at least some of its members and develop training to support that end, alongside the traditional method of having individuals learn on the job.

What measures can be taken to make the relationship between Canada's intelligence agencies and government decisions makers more effective and efficient?

Strengthening the Intelligence-Policy Nexus

In research conducted between 2018 and 2019, my colleague Thomas Juneau and I found that since the early 2000s there has been an important improvement in the relationship between the intelligence and policy communities in Canada, but there remains significant room for improvement.¹³

- Intelligence literacy in the policy community remains low. Individuals spoke to us about receiving products that seemed to come from a “black box” – not knowing how intelligence producer were made or where they were coming from. There is also a sense that the policy community needs to improve its strategic culture, to better understand how their roles and responsibilities impact Canadian security – broadly understood.
- Policy literacy in the intelligence community also remains low. Intelligence analysts and managers do not understand their clients or their priorities as well as they should. This means products are not crafted in ways that speak to them, are too long

¹² Blair Rhodes, “Halifax man acquitted on charge of violating Syria trade sanctions”, 10 December 2020. <https://www.cbc.ca/news/canada/nova-scotia/halifax-man-acquitted-on-charge-of-violating-syrian-trade-sanctions-1.5835784>

¹³ Juneau and Carvin, *Intelligence Analysis and Policy Making*



or are not timely. Unfortunately, there are not many opportunities for intelligence analysts to learn about the policy making process.

Strains and pressures between intelligence agencies and policy makers are necessary and exist in all Western countries. However, we find that our allies do more to help ameliorate some of the negative externalities of these tensions. This includes:

- training analysts to produce content that speaks to their policy clients and their interests in ways they get products which speak to what they need to know, even if it is not what they want to hear.
- utilizing secondments between the intelligence and policy communities that strengthen both. (Too often secondments are used to get rid of problematic employees rather than enhance the careers of the strongest ones.)¹⁴
- educating consumers of intelligence products by providing “Intelligence 101” briefings on what intelligence is, what it can do and its limitations.¹⁵
- Increasing interactions between policy makers and intelligence analysts at all levels, including interdepartmental meetings, that can focus discussions, improve understanding and build trust and personal ties.¹⁶

It is advisable for the Canadian national security and intelligence community to adopt these steps.

It is also important to find ways to make it easier for policy analysts and senior clients to access classified information:

- At present, to access highly-classified information, individuals must leave all their electronic devices behind to enter a secure location, that is often in another room, floor in their building or in another building altogether. They then must navigate intelligence portals which can contain hundreds if not thousands of messages to find what they are looking for.
- Once they read this information, there are strict limits on sharing what they know although they may be able to act on it.
- The government needs to invest and modernize the way we communicate and present classified information to the policy community. While there may be technological solutions to this problem, the government should also explore opportunities to improve its use of open-source information and the “traffic light protocol” used by the Canadian Centre for Cyber Security (discussed further below).¹⁷

¹⁴ Juneau and Carvin, *Intelligence Analysis and Policy Making*, pp. 67-70.

¹⁵ Juneau and Carvin, *Intelligence Analysis and Policy Making*, p. 153.

¹⁶ Juneau and Carvin, *Intelligence Analysis and Policy Making*, p. 154.

¹⁷ Stephanie Carvin, “Canadian National Security Operations During COVID-19”, in Leah West, Thomas Juneau and Amarnath Amarasingam, *Stress Tested: The COVID-19 Pandemic and Canadian National Security*, Calgary: University of Calgary Press, 2021. pp. 107-126. pp. 118-119. Designed to facilitate



Better coordination of institutions

In the past the Canadian intelligence and national security community has been characterized by a weak centre and immature coordinating structures. Based on research conducted with members of the community in 2018-2019, there are several consequences to a lack of centralization/coordination:

- the work of departments and agencies is siloed;
- the community is often unable to speak with one voice in a way that can shape working-level and higher-level discussions;
- intelligence assessments are not connected to the process of developing and implementing policy;
- there is a lack of coordination between the international and domestic aspects of an issue;
- personalities have a disproportionate impact on the success and failures of intelligence analysis. Rather than institutionalized processes and procedures, intelligence products are distributed and consumed based on the personal interest of senior leaders.¹⁸

In addition, as has been identified throughout the PIFI hearings, there appears to have been difficulties in delivering intelligence “up the chain”. For example, both the Rouleau and Johnston Reports found the government is missing effective protocols on information sharing, intelligence gathering, and distribution.¹⁹

Recent steps to improve this situation include the creation of new DM and ADM committees on national security, intelligence and operations. In addition, a new cabinet committee, the National Security Council (NSC), which is intended to serve as a “forum for strategic decision-making and for sharing analysis of intelligence in its strategic context,”²⁰ will

information sharing between the government, the private sector and other key stakeholders, the protocol uses four colours to indicate information sharing boundaries for recipients of the information. While information flagged as “red” may not be shared beyond the direct recipient, “yellow” information is on a need-to-know basis, “green” may be shared with peers and partner organization and “white” information may be distributed without restriction. Cyber Centre employees argue that this allows them to provide more meaningful advice and information outside of government

¹⁸ Juneau and Carvin, *Intelligence Analysis and Policy Making*, pp. 14-23.

¹⁹ Public Order Emergency Commission, *Report of the public inquiry into the 2022 public order emergency*, Volume 3: Analysis (part 2) and recommendations. POEC, February 2023. pp. 277 Available at: <https://publicorderemergencycommission.ca/final-report>; David Johnston, *First Report - The Right Honourable David Johnston, Independent Special Rapporteur on Foreign Interference*. Government of Canada, 2023. p. 18. Available at: <https://www.canada.ca/content/dam/di-id/documents/rpt/rapporteur/Independent-Special-Rapporteur%20-Report-eng.pdf>.

²⁰ Prime Minister of Canada, “Cabinet Committee Mandate and Membership”, 19 September 2024. <https://www.pm.gc.ca/en/cabinet-committee-mandate-and-membership#national-security-council>



hopefully better inform Cabinet on national security issues when major decisions are being undertaken. The NSC is supported by a secretariat, led by an assistant secretary.

These recent measures are welcome, but the government should take further steps to enhance coordination and cooperation. In particular, the role of the NSIA should be strengthened and their ability to coordinate the national security and intelligence community further codified through a legal instrument, ranging from an order-in-council through to formal legislation.²¹ Formally establishing these NSIA functions would also contribute to reducing the oversized impact of personalities on the flow and use of intelligence in government decision making.

What measures can be taken to improve the communication of intelligence and the understanding of the implications of foreign interference threats with external stakeholders such as political parties and candidates? How should the tension between providing information specific enough to be meaningful and protecting the operational and security imperatives that require limits on information-sharing best be resolved?

Open-source information

Given the importance of raising awareness of the risks of foreign interference, and the passage of the *Countering Foreign Interference Act* (CFIA, Bill C-70), significant attention has been paid to developing ways to share intelligence outside of the Canadian intelligence and national security community. This is an important conversation and developing processes around new authorities to share intelligence will be fundamental to protecting Canadian institutions and affected communities.

Yet it is unlikely that the intelligence sharing processes and authorities in the CFIA will be sufficient for raising general awareness of the issues and challenges of foreign interference. In this way, the government should explore other options to communicate information about national security threats, particularly the use of open-source intelligence (OSINT).

Most of the information contained in intelligence products can probably be found in some kind of open-source information.²² Therefore open-source products could be used to better

²¹ An order-in-council is the most expedient way of accomplishing this and it would allow for more flexibility over time as these institutions are become embedded in the decision-making processes of cabinet. On the other hand, formal legislation creates a more permanent approach, formalizing the arrangement and allowing for a greater sense of stability/predictability for the community. Both approaches have their trade-offs, with the former being more expedient and flexible and the latter being more permanent.

²² Juneau and Carvin, *Intelligence Analysis and Policy Making*, pp. 126-128



communicate with those without clearance, particularly in cases where specific threats do not need to be communicated but better general awareness is needed.

The Canadian intelligence and national security community was turned to the use of OSINT during the COVID-19 pandemic but was able to develop useful products that were able to be distributed across government and other key stakeholders.

However, Canada should be ambitious when it comes to using OSINT, including setting up a centralized body to coordinate OSINT collection and analysis across the Canadian intelligence community. To be most effective, this body should:

- have the mandate to develop and share OSINT across all levels of government;
- become the federal policy leader and centre of excellence for OSINT collection, training, and analysis;
- work to improve coordination and breaking down current OSINT silos, it would also crucially enhance Canada's OSINT culture and capacity;

This body may be best located in the Integrated Terrorism Assessment Centre, albeit with a mandate change, and possibly under an enhanced NSIA role/office.²³

Learning to communicate with affected communities

Investigations around foreign interference require conversations with individuals of Chinese or Asian dissent. This comes at a time when hate crimes against Asian and South Asian Canadians have surged, particularly in the wake of COVID-19.²⁴ Sensitivity to this reality is integral to Canada's approach to foreign interference and it must be reflected into operations of those institutions tasked with national security investigations.

The missing "Lessons Learned": Finding the right approach to this issue is confounded by the fact that the Canadian intelligence and national security community has never conducted a "lessons learned" examination of the practices it utilized in the post-9/11 era, especially when it comes to community engagement. For years, equity deserving communities, particularly the Muslim community, have expressed concerns over certain practices, such as "door knocking" and where officers show up to places of work

²³ Arguments in this section based on Leah West and Stephanie Carvin, "Opening Hearts and Minds: Canada and the Challenge of Using Open-Source Information in National Security Operations and Analysis", in Norman Hillmer, Philippe Lagassé, Vincent Rigby, *Canada Among Nations 2023: Twenty-First Century National Security*, Cham: Palgrave, 2025. (Forthcoming)

²⁴ Vanessa Balintec, "2 years into the pandemic, anti-Asian hate is still on the rise in Canada, report shows", 3 April 2022. <https://www.cbc.ca/news/canada/toronto/2-years-into-the-pandemic-anti-asian-hate-is-still-on-the-rise-in-canada-report-shows-1.6404034>; Josiah Sinanan, "South Asian newcomers to Canada say online hate is taking a toll", CBC News, 22 June 2024. <https://www.cbc.ca/news/canada/windsor/south-asian-newcomers-to-canada-say-online-hate-is-taking-a-toll-1.7243057>.



unannounced. It is concerning that the intelligence and national security community does not necessarily understand the impact of these institutionalized routines on those who were most likely to experience them.²⁵ Moreover, as combating foreign interference requires national security engagement with different communities, we need to ensure that new threats are not managed with old and potentially flawed practices.

While there was strong support for Bill C-70 and for the government to take action on foreign interference among ethnic and equity deserving groups in Canada, it is also worth noting that some of the chief opposition came from other groups, particularly Muslims and Sikhs (also foreign interference targets), who fear enhanced powers for national security agencies will ultimately be used against them.²⁶

Adjusting practices: Even more “mundane” practices may have to be adjusted to accommodate counter-foreign interference operations/investigations. For example, the national security and intelligence community often uses roundtables and meetings to engage with communities and hear their concerns. Increasingly, these forums are also used to brief key stakeholders, such as universities, research institutions and key businesses about espionage and foreign interference. By some accounts, these meetings are in-demand and well-received.²⁷ However, it is not clear that, in an online age, that such an approach will work when attempting to do outreach to ethnic communities on foreign interference, especially where individuals may be afraid to be seen meeting with state security officials or be concerned about surveillance.

A sophisticated approach is needed when engaging with ethnic communities and equity deserving groups, especially in a digital age. Security agencies need to find and make available safe and secure channels for individuals to contact them, especially if they feel they are being watched or monitored.

Developing subject matter expertise: Unfortunately, the generalist model used by national security and intelligence agencies (discussed above), and the lack of specialists within these organizations, may be hampering efforts at outreach. Diaspora and equity deserving groups face a complex array of challenges and have their own political debates and discussion. Understanding this context is extremely important for countering foreign interference but cannot be taught overnight or simply “on the job” in a matter of weeks.

Therefore, the government should:

²⁵ Navaid Aziz and Stephanie Carvin, “As Canada’s national security agency looks forward, it must also look back”, *Globe and Mail*, 16 July 2021. <https://www.theglobeandmail.com/opinion/article-as-canadas-national-security-agency-looks-forward-it-must-also-look/>

²⁶ Raffy Boudjikianian, “Groups representing minorities say they’re alarmed by foreign interference legislation”, 23 July 2024. <https://www.cbc.ca/news/politics/groups-representing-minorities-say-they-re-alarmed-by-foreign-interference-legislation-1.7271916>

²⁷ CSIS, *Public Report 2020*, 2021. p. 18.



- Work with the national security and intelligence community to either develop expertise on cultural practices and language, or find ways to work with subject matter experts in order to better understand the challenges faced by diaspora and equity deserving groups in Canada;
- Produce nuanced and carefully translated materials about foreign interference in multiple languages – not simply English and French – that can be obtained in secure ways.