Summary Report

Author: Maria Robson-Morrow, Harvard University. *Please note that the views expressed here are my own and do not reflect those of my employer.*

Panel Theme: Canada's National Security Apparatus

Key Issues:

This response focuses on how to effectively communicate security intelligence information on foreign interference to external stakeholders, the public, and vulnerable communities. The eight years of research underpinning my assessments and recommendations has focused on information sharing and intelligence sharing with non-traditional partners. There are two underlying principles in my response.

First, the "crown jewels" are not always in the hands of governments, and certainly not always in the hands of the security agencies. Therefore, Canada's National Security Apparatus must provide mechanisms for effective, trusting two-way engagement with external parties. An effective national security apparatus needs to engage external entities as partners, not just as victims.

Second, Canada is not alone in this challenge. Our Five Eyes intelligence-sharing partners have models that can be instructive when applied in a Canadian context.

Assessment:

This response proceeds by examining three key categories of engagement with external parties:

1. Duty to Warn/Duty to Inform
2. External engagement models that focus on foreign interference
3. External engagement models for information sharing on security threats more broadly, and the characteristics of effective engagement across these models

First Category of Engagement: Duty to Warn/Duty to Inform

Most of the Five Eyes countries do not have a formal duty to warn, outside of their law enforcement entities. The partner that does is the United States. Duty to warn is enshrined in U.S. Intelligence Community Directive (ICD) 191. While it applies to threats to life, its parameters of how to warn and when are instructive beyond the specific type

of threat. The Directive stipulates that "An [Intelligence Community] element that collects or acquires credible and specific information indicating an impending threat of intentional killing, serious bodily injury, or kidnapping directed at a person or group of people (hereafter referred to as intended victim) shall have a duty to warn the intended victim or those responsible for protecting the intended victim, as appropriate. This includes threats where the target is an institution, place of business, structure, or location."[1]

ICD 191 has several salient aspects. First, it is very specific. Second, it is available for the public to read and understand the obligations and constraints of their intelligence agencies. Third, it includes an obligation to warn those responsible for protecting the victim, not just the victim. Fourth, it is explicit that tearlines—the information that is approved for unclassified sharing—must omit information that would compromise sources and methods, which addresses the "intelligence-to-evidence" challenge. Fifth, it provides conditions under which the duty to warn can be waived, including if: warning is simply not possible; the intended victim already knows; they are only at risk due to participating in an insurgency or other armed conflict; evidence strongly suggests that the intended victim is involved in terrorism, drug trafficking, assassinations, or violent crimes; or there are unacceptable risks to sources, methods, or personnel.[2]

Crucially, these guardrails do not serve as a crutch to avoid warning. On the contrary, Duty to Warn is frequently acted on and underpins considerable external engagement. Warning is required and the expectation is that information will be shared with appropriate safeguards in place.

In Canada, responsibility for warning has historically been in the hands of the RCMP. However, the "Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians," issued by the Minister of Public Safety in May 2023, changed this landscape by requiring CSIS to "ensure that parliamentarians are informed of threats to the security of Canada directed at them," and authorizing direct disclosures.[3] Added to this is now Bill C-70's amendment to the CSIS Act to allow "disclosures to partners to build resiliency to threats."[4]

---

[1] ODNI, *ICD 191,* U.S. Government, 21 July 2015, https://www.dni.gov/files/documents/ICD/ICD-191.pdf.
[2] *ICD 191,* https://www.dni.gov/files/documents/ICD/ICD-191.pdf, pp. 2-3.
[3] Public Safety Canada, "Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians", Government of Canada,16 May 2023, https://www.publicsafety.gc.ca/cnt/trnsprnc/ns-trnsprnc/mnstrl-drctn-parl-secure-en.aspx and Catharine Tunney, "CSIS officially directed to share more information with Parliamentarians under threat", *Globe and Mail,* 16 May 2023, https://www.cbc.ca/news/politics/csis-ministerial-directive-1.6845542.
[4] Public Safety Canada, "Modernizing Canada's Toolkit to Counter Foreign Interference", Government of Canada, 27 August 2024, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/frgn-ntrfrnc/mdrnzng-tlkt-frgn-ntrfrnc-en.aspx.

These two changes represent a key step forward; however, their guidance is quite open-ended. There is value in flexibility and discretion, but there is often also value in specificity. General language can prompt confusion, obfuscation, and concerns about preferential treatment. Furthermore, not providing exceptions for the duty to inform immediately invites noncompliance; in some cases, warning simply will not be possible. ICD 191 is specific that in certain situations, warning cannot reasonably be expected, but overall, it is required.

Thus, CSIS currently has a requirement to warn and the ability to engage; however, implementation is a challenge. While some flexibility and discretion are always necessary, drawing on specific parameters from partner countries, such as ICD 191, can be helpful.

Second Category: Engagement Models on Foreign Interference

The policy roundtable preparatory document asked whether and how Canada's national security and intelligence agencies should communicate with the public on foreign interference threats and how to protect themselves. This response contends that yes, they should, and our closest allies have relevant examples of how it can be done.

In 2018, Australia established the Counter Foreign Interference Coordination Centre. The Centre supports the National Counter Foreign Interference Coordinator, who sits within the Department of Home Affairs. The Centre has a "whole of government approach" and works with "the private and civil sectors, the wider community, and with international partners," with the mission to "strengthen Australia's response and resilience to foreign interference."[5] The Australian approach includes a hotline for reporting possible foreign interference, and two-way engagement with external partners.

The U.S. equivalent is the Foreign Malign Influence Center, within the Office of the Director of National Intelligence, activated in 2022.[6] The Foreign Malign Influence Center was established because of a recognition that foreign interference into democratic processes is ongoing, and needs to be tackled 365 days a year, every year, rather than by election-specific task forces. It has two particularly noteworthy aspects: (1) a public Notification Protocol that includes notifying victims and also issuing public advisories.[7] There is a risk calculation to ensure that notification will be beneficial rather

---

[5] Department of Home Affairs, Australian Government. *Tri-fold: Counter Foreign Interference Coordination Centre.* 2024. https://www.homeaffairs.gov.au/nat-security/files/tri-fold-xsect-cficc.pdf.
[6] ODNI, "FMI Primer, Vol. 1", U.S. Government, April 2024, https://www.dni.gov/files/FMIC/documents/products/04-25-24_Report_FMI-Primer-Public-Release.pdf and "FMI Primer, Vol. 2", October 2024, https://www.dni.gov/files/FMIC/documents/products/10-18-24_Report_FMI-Primer-Vol-2-Public-Release.pdf.
[7] ODNI, "Overview of the Process for the Executive Branch to Notify the Public and Others Regarding Foreign Malign Influence and Interference Operations Targeting U.S. Elections", U.S. Government, https://www.dni.gov/files/FMIC/documents/Overview_of_the_Process_for_the_Executive_Branch_to_Notify_the_Public.pdf.

than amplifying the adversary's message or otherwise helping the adversary. (2) External engagement that includes information exchanges, not just pushing information. Participants are external experts, government partners, industry, and civil society.

Both of these models are nascent and evolving, and international benchmarking is key to success.

Third Category: Engagement Models for Security Information Sharing – Characteristics of Effective Engagement

Beyond engagement models specific to foreign interference, there are information-sharing models that facilitate two-way engagement and build trust that are worth examining closely.

One exemplary model of security information sharing is the Overseas Security Advisory Council (OSAC), which has operated since 1985 and sits within the U.S. State Department's Diplomatic Security Service with a mission to promote security cooperation "by fostering a global network of security professionals who exchange timely information and security best practices to mitigate risks to U.S. interests worldwide."[8] This model encompasses non-profit organizations and non-U.S. companies, including Canadian companies, with a presence in the U.S. and relevance for U.S. persons' security. The relevance of the OSAC model appeared both in my interview research and a Public-Safety-funded Conference Board of Canada 2017 study that invoked OSAC as an information sharing model worth emulating in Canada.[9]

Successful models build trust and facilitate a culture of engagement that goes beyond what is obligated by law. As the 2017 study states, "there is a danger of overstating the restrictive aspects of the law while not fully acknowledging the importance of organizational culture."[10] Part of the Overseas Security Advisory Council's success is that it empowers non-government partners to drive the agenda rather than dictating what government believes is of interest.

In Australia, the Australian Security Intelligence Organisation (ASIO)'s external outreach branch, ASIO Outreach,[11] adopted lessons from the OSAC model, and has had success

---

[8] Department of State, "OSAC", U.S. Government, https://www.osac.gov/About/AboutUs.
[9] Conference Board of Canada, *The State of Information and Intelligence Sharing in Canada,* 2017, https://epe.lac-bac.gc.ca/100/200/300/conference_board_canada/briefing/2017/8487/8487_Intelligence-Sharing-in-Canada_BR.pdf.
[10] *State of Information and Intelligence Sharing in Canada,* https://epe.lac-bac.gc.ca/100/200/300/conference_board_canada/briefing/2017/8487/8487_Intelligence-Sharing-in-Canada_BR.pdf, pp. 1.
[11] Australian Security Intelligence Organisation, *Outreach,* Australian Government. https://www.asio.gov.au/outreach. There are some parallels to CSIS's Academic Outreach and Stakeholder Engagement: https://www.canada.ca/en/security-intelligence-service/corporate/academic-outreach.html.

with external threat information sharing with non-governmental actors who want to engage.

Recommendations:

This report concludes with the following recommendations for Canada's national security apparatus.

1. **Proactively engage external parties in way that recognize that they are partners, not just victims; they hold key pieces of the security puzzle. Engagements should have these four key characteristics:**[12]
    a. **Repeat engagement** rather than one-off interactions, when possible. This builds credibility and trust.
    b. **Two-way interaction.** Defensive briefings have a role to play; however, two-way engagement builds trust and enables recipients of information to share their own pieces of the puzzle.
    c. Leveraging already-trusted organizations. The Conference Board study revealed a focus on associations as more trusted than sharing relationships with government,[13] and when government engaged in those associations, they were more likely to have success. This is corroborated by my research. Effective government partners engage with pre-existing privately-driven organizations when possible rather than adding duplicative mechanisms.
    d. Building mutual understanding of each other's priorities and capabilities. A meeting that participants see as a waste of time can prompt long-term disengagement. Fostering a better understanding of each other's knowledge, capabilities, priorities, and pain points builds trust and makes for better information exchange and threat mitigation. Partners need to know what government can and cannot do. This is particularly true of engaging civil society, diaspora groups, and industry.

2. **Raise awareness of the role of intelligence, and Canada's intelligence services, by proactively sharing *successes*.** A culture of secrecy can lead to a lack of awareness of intelligence services—until disaster strikes. The Canadian public is disproportionately aware of intelligence failures and scandals, rather than quiet successes in thwarting threats to Canadians. Intelligence risks being the goalie; people rarely remember the shots that do not go-in. Disclosing intelligence operations with a clear link to public safety, such as the 2006 thwarting of the

---

[12] Robson, Maria A. *Beyond borders: how public and private actors institutionalize intelligence cooperation.* Dissertation. Northeastern University, 2021. https://doi.org/10.17760/D20420718.
[13] *State of Information and Intelligence Sharing in Canada,* https://epe.lac-bac.gc.ca/100/200/300/conference_board_canada/briefing/2017/8487/8487_Intelligence-Sharing-in-Canada_BR.pdf, pp. 24.

Toronto 18 terror plot,[14] can build credibility. This report recommends encouraging culture of proactive disclosures and revealing intelligence outcomes that are relatable to the Canadian public.

3. **Leverage open-source information to protect classified information:** The policy roundtable preparatory document asked how to balance the need for specificity with the security imperative to protect information. Sometimes the answer is to emphasize sharing as much substance as possible while safeguarding sources and methods, as in ICD 191. However, a more satisfying answer is: when possible, using open-source information to mask classified information. When the White House proactively disclosed intelligence to reveal Vladimir Putin's February 2022 plan to invade Ukraine, the U.S. National Security Council was able to point to open-source geospatial information to mask clandestine sources that had directed them to similar conclusions.[15] History is replete with examples of one source being used to protect another—often human agents whose lives would be at risk. Intelligence agencies can draw on open-source information even if their original information is through classified channels, thereby helping with the intelligence-to-evidence problem.

4. **Focus on improving horizontal engagement at all levels of the intelligence apparatus, not just the top.** Engagement needs to focus on all levels of the intelligence service, not just the Director of CSIS and other high-level positions. Productive engagements often taken place at the operational level through horizontal engagement with external parties.

5. **Examine partner countries' models and adapt their best practices.** Our intelligence partner countries have models that are instructive, in three categories: duty to warn, foreign interference centers, and public-private engagement models. As examined above, models such as Intelligence Community Directive 191 (Duty to Warn), the U.S. Foreign Malign Influence Center, Australia's Counter Foreign Interference Coordination Centre, ASIO Outreach, and the U.S. State Department's Overseas Security Advisory Council have important characteristics that are worth examining and potentially applying in a Canadian context.

---

[14] CBC, "Toronto 18: Key events in the case", 4 March 2011, https://www.cbc.ca/news/canada/toronto-18-key-events-in-the-case-1.715266.

[15] Julian Barnes and Adam Entous, "How the U.S. Adopted a New Intelligence Playbook to Expose Russia's War Plans", *New York Times,* 23 February 2023, https://www.nytimes.com/2023/02/23/us/politics/intelligence-russia-us-ukraine-china.html.