Summary Report

Author: Daniel Jean, Retired Deputy Minister, Former National Security and Intelligence Advisor to the Prime Minister and Deputy Minister Foreign Affairs; continued interest for these issues with multiple affiliations such as Honourary Senior Fellow at GSPIA of University of Ottawa and board member of the Conference of Defence Associations.*

Panel Theme: Canada's National Security Apparatus

Capturing the challenges

- The Inquiry's proceedings have so far raised at least 6 issues relevant to the national security apparatus:
  1) The absence of a national security culture, which affects strategic assessment and calls into question our legal instruments and approaches, especially during one-off crises.
  2) The challenge of developing quality intelligence products with clearly stated reliability.
  3) Distribution of products to key civil servants and relevant policy-makers, guiding action where necessary and possible.
  4) A systemic approach so that relevant products are brought to the attention of these same officials and key policymakers, with documented confirmation of their awareness.
  5) In a world where the crown jewels are increasingly outside of the government, foster a fundamental cultural shift to better alert and support Canadians in countering foreign interference.
  6) Horizontal governance among officials and in Cabinet, where issues and options are discussed in depth to ensure greater coherence and coordination.

- Let's review these 6 challenges and possible improvements while addressing some of the questions addressed to the panel.

1) The absence of a national security culture, which affects strategic assessment and calls into question our legal instruments and approaches, especially during one-off crises.

Responds in part to question 1

* Translation

1. ***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? Do they have the authorities and tools they need to effectively counter foreign interference? What more can be done to improve Canada's capacity to detect and counter the threat?***

Historically, our laws have often been amended following crises. For example, the McDonald Commission [1] led to the legislation creating CSIS, terrorist acts led the National Security Act of 2015[2] and the current debate on foreign interference has led to the accelerated adoption of Bill C-70[3].

The issues of the day that concern citizens have rapidly regained attention, undermining strategic assessment and attempts by various governments to create more space for these strategic discussions. The recent creation of a National Security Council is a new attempt, but it is still too early to judge. The recently passed Bill C-70 corrects many of the shortcomings of the 1984 CSIS Act, both in terms of bringing it into the digital age and allowing it a more active role in articulating the threat to external actors. The measure to regularly update the Act is encouraging, but should be more than a procedural exercise.

2) Developing quality intelligence products with clearly stated reliability.

- The Commission's proceedings have highlighted the challenge of developing quality intelligence products with clearly defined levels of reliability. It is striking to note how different actors could interpret the same intelligence documents differently. Consider in particular the recent reportof the National Security and Intelligence Committee of Parliamentarians (NSICOP)[4] and those who have had access to classified material, and contrast it with recent CSIS testimony on the most egregious cases of interference, which provided important nuances[5].

In the first few weeks after the intelligence leaks, we witnessed dangerous extrapolations treating intelligence as evidence. The Op-ed of Dr Carvin in the Globe and Mail[6] was very useful to differentiate these terms.

---

[1] https://www.thecanadianencyclopedia.ca/en/article/royal-commission-on-inquiry-into-certain-activities-of-the-royal-canadian-mounted-police

[2] https://www.justice.gc.ca/fra/jp-cj/sn-ns/lat15-ata15.html

[3] https://www.noscommunes.ca/committees/fr/SECU/StudyActivity?studyActivityId=12773790

[4] CPSNR, Rapport spécial sur l'ingérence étrangère dans les processus et les institutions démocratiques du Canada, 3 juin 2024

[5] https://www.cbc.ca/news/politics/foreign-interference-csis-1.7336005

[6] Stephanie Carvin, The Globe and Mail, Opinion: What are we talking about, when we talk about intelligence?, 3 mars 2023

If sometimes an intelligence element, for example an unequivocal intercept of a conversation could, if it is possible to use it without endangering sources, methods or investigations, be used as evidence --- Most of the time, intelligence is based on information of varying degrees of reliability.

- Intelligence gathering and analysis must remain independent, and inform the development of strategies, public policies and operations in a neutral way. However, intelligence cannot be developed in a "vacuum". Regular exchanges between targeted audiences and the authors of the intelligence are essential to ensure that the intelligence product benefits from all the desired value-added diligence.
- With regard to the quality and reliability of intelligence, the example cited of the different interpretations should enlighten our intelligence services on the need to get into the minds of audiences who are not intelligence experts, and ensure that the document is clear on what can be established with certainty versus the hypotheses and different degrees of reliability on which they are based.
- Much progress has been made in the national security community's ability to work horizontally on different issues, but intelligence work is still too compartmentalized.

3) Distribution of products to key civil servants and relevant policymakers, guiding action where necessary and possible.

Focuses largely on questions 2 and 3

Q2 ***What measures can be taken to make the relationship between Canada's intelligence agencies and government decision makers more effective and efficient?***

Q3 ***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? Can amendments to section19 of the Canadian Security Intelligence Service Act in Bill C-70 be expected to improve information sharing? What will they address and what will they not address?***

While it is crucial to increase the quality of intelligence products, it is equally important to ensure that they are brought to the attention of the relevant audiences, and that the most important ones are brought to the attention of the highest echelons of these audiences, either by reading or by written or oral briefing of their summaries.

- We refer to different target audiences in the plural, because in today's complex world :The security and intelligence community must constantly work with other ministries and agencies, for example economic ministries on economic security issues, or social

ministries/agencies on issues such as disinformation, or election integrity institutions such as the Commissioner of Canada Elections.

- The Commission's findings on interference reinforce the importance of parliamentarians and political parties alike being regularly informed about the evolution of relevant threats. As mentioned above, this information should inform their codes of conduct.

4) **A systemic approach so that relevant products are brought to the attention of these same officials and key policymakers, with documented confirmation of their awareness.**

The Commission's proceedings have revealed that some key information may not have been sent out, or may not have received the necessary attention from those who received it, given the multitude of issues at stake on a daily basis.

- We cannot expect government leaders internally, or key external players such as parliamentarians or political parties, to spend time reading every intelligence product.However, it is essential that security clearances are in place for the most important players, and that they create the space for the essential elements of threat intelligence that require their attention.
- These exchanges should be carefully documented to promote system-wide accountability.

5) **In a world where the crown jewels are increasingly outside of the government, foster a fundamental cultural shift to better alert and support Canadians in countering foreign interference.**

Responds particularly to question 6,

Q6 Should *Canada's national security agencies better communicate with the public about the threat of foreign interference and how to protect themselves against it and, if so, how?*

But also, to question 4.

Q4 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?*

In an environment where the crown jewels and the interference targets by foreign states or their proxies are more and more outside government[7]—For example:

[7] https://utorontopress.com/9781487550752/intelligence-cooperation-under-multipolarity/ , conclusion

- sensitive technologies/research in the private sector or in universities/institutes.
- manipulation via systemic disinformation that can undermine confidence in democratic institutions.
- monitoring, harassment and intimidation of diasporas to silence criticism.
- the fundamental role of political parties in our democracy.
- the fact that some of these crown jewels and vulnerabilities are found in various levels of government (provinces, territories, municipalities, indigenous governments).

The evolution of this environment means that our security apparatus needs to know more about these different players, and to forge bonds of trust with them. It must make good use of existing and new authorities (C-70) to provide more information about the threat and its forms, while protecting sources, methods and investigations.

This calls for a profound cultural change, which means adjusting recruitment, training and follow-up methods to foster organizational behavior adapted to this new reality.
A few comments on what it means for key institutional actors:

- Because the cyber threat is significant for our democracy, infrastructure and critical sectors, the CST, once one of the most secretive organizations, has already begun this shift, but needs to go further and move from threat awareness to resilience.
- The shift required is considerable for CSIS, which until now has been handcuffed in its external engagement by outdated legislation but whose culture is deeply rooted in the old environment.
- Resolve the conflict over the RCMP's ability to fully play its federal policing role when so much of its attention and resources are monopolized by contract policing.

While the protection of methods, sources and investigations may be a barrier to external sharing, risk aversion is much greater in Canada than elsewhere. We also underestimate what can be achieved with open sources. It is imperative to make this shift.

6) **Horizontal governance among officials and in Cabinet, where issues and options are discussed in depth to ensure greater coherence and coordination**.

Offers additional avenues to respond to question 1.

While not perfect, horizontal governance among officials in the national security apparatus has made significant progress since the creation of the NSIA position in 2003.

- The agility to respond in a coherent and coordinated fashion to crises via the Deputy Ministers Operations Committee (DMOC) has reached an encouraging level of maturity and the creation of the Incident Response Group (IRG) has allowed a natural extension to Cabinet.
- The aspect of decompartmentalizing intelligence while protecting its independence that I mentioned earlier is the next step that needs to be taken.
- In terms of policy development, there are reasonable efforts to promote healthy discussions in the development of policies related to the government's mandate, while anticipating emerging issues. Significant progress has also been made in integrating external players, such as economic ministries/agencies when discussing economic security (Appendix 2).
- The lack of appetite and time for more strategic discussions remains a challenge. The creation of the National Security Council offers an opportunity, but it is too early to judge.

The **role of the NSIA** is key to this horizontal governance both among officials and as a key link with the Prime Minister and Cabinet. There are no major obstacles to codifying the NSIA role in law. However, unless we revisit the Westminster model where responsibilities remain with Ministers and their institutions, this will undoubtedly articulate the role mirrored by the Privy Council Office (PCO) i.e:

- Independent advice to the PM.
- Support and advice to Cabinet.
- « Convening role » to promote coherence and coordination of public policy and operational efforts.

We grant much importance to the role while the **attributes** of the holder are probably as important. The NSIA must be someone:

- Experienced and respected by their peers, so they can promote coherence and coordination, and challenge assumptions or proposals.
- Capable of providing « fearless advice » to key audiences (PM, Cabinet).
- Who brings added value both to the security apparatus and to key audiences (PM, Cabinet). S/he is the conjunctive tissue but cannot be the unilateral "amplifier" of one or the other.

Appendix 1 Recommendations

R1- Political institutions and the national security apparatus must responsibly raise Canadians' awareness of the threat of foreign interference and what it means for our prosperity and democratic freedoms, and engage them in ongoing prevention and resilience efforts.

R-2 The intelligence-gathering process, while remaining independent and neutral with regard to policy development or operations, must be decompartmentalized and involve clients in order to benefit both from the challenge and verification of facts and hypotheses, and from the added value of additional information.

R-3 The divergent interpretations made by different actors after reading the same intelligence products in the recent debate on foreign interference should enlighten our intelligence services on the need to get into the minds of audiences who are not intelligence experts, and ensure that the document is clear on what can be established with certainty versus the assumptions and varying degrees of reliability on which they are based, and in language suitable for an external audience.

R-4 Given that the Commission's proceedings have revealed that some key information may not have been sent, or may not have received the necessary attention from those who received it due to the multitude of issues at stake on a daily basis, it is essential that security clearances are in place for the most important players (officials, ministers, parliamentarians and political parties) and that they create the space for the essential elements of threat intelligence, which require their attention, to be communicated to them. These exchanges must be carefully documented to promote the accountability of the system as a whole.
R-5 In an environment where the crown jewels and the targets of interference by foreign countries or their proxies are increasingly external to government, our security apparatus needs to know more about these external players, and to forge bonds of trust with them. It needs to make a major cultural shift and make good use of existing and new authorities (C-70) to provide more information about the threat and its forms, while protecting sources, methods and investigations.

Appendix 2
Short case studies illustrating good responses to the threat of foreign interference

Australia. In 2017, the Australian government realized how deep China had infiltrated various aspects of Australian society. Its efforts included election financing, influencing parliamentarians, former senior politicians, officials and private citizens, employing undisclosed foreign agents, pressuring universities through grants and donations, and acquiring sensitive technology both in the private sector and in universities. Prime Minister Turnbull brought in John Garnaut, a lawyer by trade who had become a journalist specialized on China, to work with the ASIO (Australia's CSIS equivalent) to discretely assess the situation and guide Cabinet in developing a set of measures. These measures subsequently became public (reform of electoral financing, creation of foreign agents registry, sharpening of foreign interference measures and penalties, and increased scrutiny on foreign investments)[8]. Some of the measures eventually attracted Chinese retaliation. In the last few years, the Australian Government has continued to sharpen its deterrence instruments and efforts. Recent foreign interference convictions[9] have supported the deterrence message.

Canada Economic Security In terms of economic security, Canada's response from 2015 onwards to concerns with China's acquisition of sensitive technologies or strategic resources illustrates that a concerted whole-of-government approach with targeted measures can bear fruit. It is worth remembering that the 2015 mandate letter[10] to the ISED Minister called on him to promote investment in promising sectors, but at a time when a growing percentage of foreign direct investment worldwide was coming from China. Officials from the national security apparatus and their relevant colleagues in the economic ministries worked closely to sensitize their ministers and the Cabinet to the risks of certain investments. The government responded with a succession of administrative, regulatory and legislative measures. A look at the Canada Investment Act statistics over the past seven years shows an increase in foreign investment rejections and abandonments in sensitive sectors. The various measures send a message that Canada is not open to foreign investment that could be injurious to national security, and Bill C-34, which received Royal Assent on March 22, 2024, will sharpen many of these tools[11].

[8] John Garnaut, How China Interferes in Australia And How Democracies Can Push Back, Foreign Affairs, 9 mars 2018
[9] https://www.afp.gov.au/news-centre/media-release/first-sentence-foreign-interference-handed-down
[10] https://www.pm.gc.ca/fr/lettres-de-mandat/2015/11/12/archivee-lettre-de-mandat-du-ministre-de-linnovation-des-sciences-et
[11] ISDE, Document d'information mis à jour : Loi modifiant la Loi sur Investissement Canada, 27 mars 2024