Summary Report

Author: Lex Gill, Senior Fellow, Citizen Lab, Munk School of Global Affairs, University of Toronto

Panel Theme: Canada's National Security Apparatus

Key Issues:

1. This report summarizes my comments in response to the questions listed in subsection 2.6 of the Preparatory Document on the Policy Aspect of the Public Inquiry into Foreign Interference, with a focus on:

    - Question 1 (adequacy of legal authorities, technical capabilities and resources)
    - Question 5 (public perception and trust in Canada's national security agencies)
    - Question 6 (communication with the public on the threat of foreign interference)

2. My comments also address the additional questions sent by Dr. West prior to the panel regarding Canada's knowledge regarding diaspora-specific factors in this arena, potential gaps in Canada's response to foreign interference and transnational repression involving vulnerable and marginalized groups, and the trust and confidence of these communities in relation to Canada's national security agencies.

3. Responses are grouped by theme below.

Assessment:

A. The *Charter* in the National Security Context

4. In response to complex problems like foreign interference, the reflex of government actors is often to demand more — more power, more funding, more resources.

5. Canadian law — and in particular the *Charter* — nonetheless imposes strict limits on the extent of permissible state power, including in the sphere of national security and intelligence. No matter how serious or pressing the state objective in question, there can be no "*Charter*-free zones" in Canadian law.

6. National security is an area that tests the limits of our constitutional infrastructure to adequately protect and safeguard fundamental rights and freedoms in Canada. The reality of serious, urgent, and complex threats creates a practical need for both rapid state intervention and far more secrecy than would be constitutionally permissible in any other area of law.

7. The powers required — or the powers that state officials have often argued are required — to combat foreign interference pose particularly acute threats to the freedoms of expression and association (section 2), the rights to liberty and security of the person (section 7), the right to privacy (section 8), and the right to equality (section 15).

8. These powers are intrusive and involve the ability to profoundly (and in some cases irreparably) impact individuals' lives. Errors and abuse can have grave consequences for individuals, their futures and their families, and can deeply undermine public confidence in our legal institutions and our justice system.

9. Options for prevention, repair and deterrence are more limited in this arena than in other areas of law. Many powers exercised by Canada's national security agencies are extremely difficult for courts to meaningfully review, the extent of disclosure to affected individuals and the ability to engage in a true adversarial process can be limited, and Canadian intelligence bodies have faced significant criticism from our courts.

10. In other words, there is simply no other area of Canadian law where the state is entitled to act with so much latitude, exercise so much power, access so much information, and impact the lives of so many people with so little scrutiny.

11. This is not meant to suggest there are no protections or safeguards in place. Indeed, the creation of the Intelligence Commissioner and the National Security and Intelligence Review Agency, as well as other reforms adopted in 2019, were

major gains in this regard. However, this remains an area where the stakes are high, the powers are extensive, review is mitigated, and the cost of getting it wrong can be incredibly serious.

12. As a result, the constitutional constraints on Canada's national security agencies must provide the starting point for the Commissioner's analysis of any new grant of statutory or executive authority in response to the challenges raised by foreign interference.

13. To this end, while obvious, it is important to reiterate that the Constitution binds the entirety of the state — including Canada's national security agencies. While the Supreme Court's approach to extraterritorial application of the *Charter* continues to leave much to be desired,[1] there is no doubt that the *Charter* applies to everything Canada's intelligence agencies do in Canada, in relation to people in Canada, and in relation to infrastructure in Canada.

14. Similarly, it is important to recall that foreign states operate through people, and so it is people in Canada who are subject to suspicion, surveillance, intelligence gathering, investigation, threat disruption measures, immigration consequences, and criminal sanction. And regardless of guilt or innocence, those people have constitutional rights.

15. This is particularly essential, as we tend to talk about the rights engaged by foreign interference through the lens of citizenship, or through the lens of the interests of "Canadians". However, with few exceptions (e.g., section 6), *all* persons in Canada are entitled to constitutional protection — not just citizens or permanent residents. There is no second-class rights framework for non-citizens as far as the *Charter*'s protections are concerned.

B. Digital Transnational Repression

16. The Commission's report is also an important opportunity to mobilize resources and build awareness regarding transnational repression in Canada, an issue with serious implications for diaspora communities and human rights defenders.

17. I would draw the Commissioner's attention in particular to a major 2022 report by Citizen Lab in this regard, which I summarize in the following paragraphs. Citizen Lab's research builds on the emerging body of work related to transnational

[1] See in particular Leah West, 'Within or outside Canada': The Charter's application to the extraterritorial activities of the Canadian Security Intelligence Service, University of Toronto Law Journal, Volume 73, Number 1.

repression and explores the ways in which it is evolving through emerging digital technologies, including the Internet.

18. Authoritarian states do not stop at their borders when attempting to suppress dissent and criticism. We know this from publicly reported cases of states working to silence or coerce nationals working on human rights issues located outside their territorial reach, including those involving Saudi Arabia, Rwanda, and China, and others.

19. The Lab's research demonstrates that digital transnational repression is an increasingly dominant form of transnational repression and is a particular threat to the rights and freedoms of dissidents and activists who are living in exile. The forms it takes are diverse, including online harassment, intimidation, threats, doxing, surveillance, use of spyware and malware, targeted leaks and hacks, and coercion-by-proxy, including through intimidation of allies, friends and family. This form of foreign interference has serious impacts on activists and dissidents in migrant and diaspora communities, including on their ability to undertake transnational advocacy work related to human rights.

20. This kind of activity is enormously common and particularly challenging because unlike direct human interactions, the digital context is seen as lower cost, scalable, more difficult to detect, and accompanied by lower risks of sanction or accountability for state actors (both because attribution is difficult and because these behaviors may be less likely to be seen as an attack on sovereignty). Women in particular face serious and distinct forms of digital transnational repression, as future research from the Citizen Lab is set to document in detail.

21. These activities are the source of a global chilling of speech and activity which disproportionally impacts certain groups in Canada — limiting not just what a person will say at a local meeting, but also what they will say and do online, and the extent to which they can meaningfully connect with collaborators and loved ones in their home country.

22. The Lab's research team concludes that support for victims and the Canadian government's response in this area has been seriously inadequate. This is in part because in Canada, the focus on foreign digital threats has overwhelmingly been related to formal democratic institutions, economic interests, and critical infrastructure.

23. The Lab's report details a series of recommendations in Section 4, many of which are relevant to the Commission's work. They include better coordination across government bodies, greater public communication, and more support for victims.

24. They also call upon the Canadian government to ensure that its own use of digital surveillance technology is transparent, lawful, and rights-respecting. More transparency from technology companies is also required regarding protocol for responding to government requests to remove content or access user information as part of efforts to respond to digital transnational repression.

25. Similarly, Canada must sanction and refuse to do business with companies that are involved in developing and selling the technology that facilitates these abuses by authoritarian regimes, including spyware manufacturers.

26. Ultimately, in order to effectively tackle foreign interference in general or digital transnational repression in particular, Canada and its national security agencies must operate with an irreproachable respect for the *Charter* and the rule of law. Legitimate concerns about abuse, overreach, discrimination, and criminalization all undermine public confidence in Canada's institutions and national security agencies, making all of us less safe.

Additional Remarks:

Regarding Amendments Included in Bill C-70

- Several panelists expressed the view that Canada's national security agencies now have sufficient legislative authority to adequately combat foreign interference following the adoption and enactment of Bill C-70 this past summer.

- It is critical to note that both the manner in which Bill C-70 was rushed through and the contents of the legislation raised serious concerns from civil society and civil liberties groups.[2] It is widely felt that this legislation was not sufficiently explained, studied, or debated, and the manner in which certain officials or experts are interpreting the scope of the new powers contained in the legislation may not ultimately withstand constitutional scrutiny.

- Given this controversy, it is critical that the Commissioner's report not operate on the assumption that the provisions contained in this complex piece of legislation or

[2] See e.g., Amnesty International Canada, British Columbia Civil Liberties Association, et. al., Joint Statement, June 6, 2024; Abdul Nakua, Bill C-70 could further erode minority rights, *Policy Options*, September 17, 2024.

the regulations that will eventually be adopted (and/or the manner in which they will be interpreted and implemented) are necessarily constitutional.

Regarding OSINT

- There were certain references to the use of open source intelligence (OSINT) during the panel session, in particular from Professor Carvin. It is important for the Commissioner to understand that while some forms of OSINT result from constitutionally innocuous and plainly public records (e.g., newspaper articles, weather reports) the vast majority of such intelligence relies on bulk collection (i.e., dragnet surveillance) of both content and metadata that may — either in relation to an individual data point or as a result of conclusions drawn from many different data points — engage serious privacy and liberty interests of those protected by the *Charter*.

- In this regard, it may be helpful for the Commissioner to refer to some of the criticism of the "publicly available information" (per the *CSE Act*) and "publicly available dataset" (per the *CSIS Act*) provisions adopted in Bill C-59, canvassed extensively in this 2017 report from Citizen Lab and CIPPIC.

- The constitutionality of these provisions has never been tested in Canadian courts. Canada's national security agencies have never clarified the manner in which these provisions are being interpreted, including (for example) the extent to which they believe these provisions apply to information sourced through social media platforms, illegal leaks, or private data brokers.

Recommendations:

1. The Commissioner's report should foreground the issue of *Charter* compliance — as well as other fundamental democratic legal principles like openness, transparency, and the rule of law — in its analysis of Canada's national security agencies' existing powers as well as regarding the potential adoption of any new statutory or regulatory authority with the potential to impact the constitutional rights of persons in Canada.

2. The Commissioner's report should not take for granted that the amendments recently adopted in Bill C-70 are constitutional, or that they will be interpreted or exercised in a constitutional manner by Canada's national security agencies. Instead, the report should invite both elected officials and members of the executive branch to convene the civil society and human rights organizations that raised concerns regarding the legislation and to engage in serious and sustained input regarding its implementation.

3. The Commissioner's report should directly address the emerging phenomenon of transnational repression, and digital transnational repression specifically. It should call for direct, concerted engagement with affected diaspora groups and proactive, transparent information sharing by Canadian officials to recognized leadership and institutions within these communities. Where appropriate, it should draw upon Citizen Lab's 2022 recommendations.