Navigating the World of Foreign Interference, Disinformation Harms to Our Democracy and Transnational Repression Effects

A playbook source for Canadians

Dr. Wesley Wark

MIGS Montreal Institute for Global Security

Canadian Heritage Patrimoine canadien

Navigating the World of Foreign Interference, Disinformation Harms to Our Democracy and Transnational Repression Effects

A playbook source for Canadians

Dr. Wesley Wark

MIGS Montreal Institute for Global Security

Canadian Heritage Patrimoine canadien

TABLE OF CONTENTS

INTRODUCTION

The importance of definitions 2

Focus on Foreign Interference 4

The Public Inquiry into Foreign Interference (PIFI) 5

The Public Inquiry and transnational repression 6

Official reports and the threat posed by TNR 12

The Disinformation Threat 13

What the PIFI said 14

The Importance of Attribution of Disinformation Campaigns 16

Insights from NGO reporting 17

CONCLUSION

Navigating the World of foreign interference, transnational, repression and digital disinformation 19

A short list of what the Government needs to do for Canadians 20

APPENDIX

About the Author 25

About the Montreal Institute for Global Security 25

INTRODUCTION

The needle of media, political and public attention in Canada swung dramatically to concerns about foreign interference and its harms to democracy starting in the Fall of 2022. Heightened attention was sparked by media reporting that often relied on leaks of selected, highly classified intelligence. This reporting in turn generated concerns about what was sometimes depicted as massive and impactful foreign interference campaigns, especially by the Peoples Republic of China. Political controversy surrounded the question of whether the government had been ignoring the threat of foreign interference, or even benefitting from it, as some opposition parties suggested.

The Government of Canada was taken by surprise by the controversy. Behind the scenes, its national security and intelligence community had been tracking the foreign interference threat for years and had even issued public reports about it in the summer of 2021, prior to the media revelations. New election security mechanisms, responding to the threat of foreign interference, with revelations about Russian interference in the US Presidential election in 2016 in mind, were designed in 2018 and implemented for the Canadian general election of 2019. The National Security and Intelligence Committee of Parliamentarians had issued a major study of foreign interference, tabled in Parliament in March 2020. It garnered little notice at the time and its recommendations were not implemented.

It should come as no surprise that, for many Canadians reading the media headlines, the idea of foreign states interfering in our democracy and in our online information spaces, seemed to be something new and foreboding, despite its long history. Since the Fall of 2022 the volume of information available about the foreign interference and disinformation threats has become voluminous and challenging to digest.

This playbook seeks to help Canadians better understand the nature of foreign interference threats and, in particular, the threat posed by disinformation and how both impact on efforts at transnational repression. The importance of such an understanding should be clear. Canadians need to have confidence in the stability and integrity of our democratic institutions and the free and fair nature of elections. Fear of foreign interference can undermine that confidence. All Canadians, including members of diaspora communities, should also expect that their government is able to offer them protection from foreign interference threats. How far that protection extends and where societal resilience comes into play are also important issues for Canadians to understand.

This playbook builds on much existing work by government agencies, Parliament, review bodies and civil society actors. The landmark investigation into foreign interference conducted by a Public Inquiry between September 2023 and January 2025 has to be considered a special reference point. The guide hopes to offer a distillation of the findings of an increasingly large body of public reporting, including from the Public Inquiry, in the hopes that it can serve as a primer for Canadians seeking to learn more about the challenges to our democracy posed by foreign Interference, disinformation, and transnational repression.

THE IMPORTANCE OF DEFINITIONS

The first place to start is with definitions of our three terms. What is "foreign interference" exactly? What is "disinformation?" What is "transnational repression?" Fortunately, we have some existing, authoritative guides that we can draw upon.

The Public Inquiry into Foreign Interference helpfully pulled together definitions of foreign interference in a document available on its website[1]. While it found variants in official usage, the Inquiry came to rely on the definition contained in the Canadian Security Intelligence Service (CSIS) Act of 1984. That definition has three key elements. To constitute foreign interference, an activity must:

- *Take place within Canada or relate to Canada*
- *Be detrimental to the interests of Canada*
- *Be clandestine, or deceptive or involve a threat to any person.*

Each of the three elements is important but the key characteristic is the aspect of clandestinity (secrecy), deception and threat. The Inquiry also noted that many definitions in use by the federal government also pointed to the actor behind foreign interference—a foreign state or proxy, and to the objective behind its use—generally to advance a foreign state's interests or strategic desires. [2]

For a definition of disinformation, we can turn to a different, but equally authoritative source. This is an infographic produced in May 2024 by the Canadian Centre for Cyber Security, a public-facing entity managed by the Communications Security Establishment.[3] Here we find that disinformation is part of a related family of terms, all of which identify different kinds of false information—colloquially "fake news" -- that circulate in our information environment. The overarching term is "misdismal" or MDM. It sounds bad, and it is. But each branch of MDM is distinguishable, and it is vital for Canadians to understand what sets this family of terms individually apart. It is all too easy to confuse them or to substitute one term for another.

This is not just a word game. The distinguishing features of each really determine how we should respond and what we might expect our government to do to combat an information threat related to foreign interference in order to protect our security and democracy.

So, we start with **misinformation**. The definition is simple:

"false information that is not intended to cause harm."[4]

Misinformation is generally circulated by people and organizations in the belief that it is true. In that important sense, misinformation is simply part of the struggle to understand and make sense of the world around us, an errant effort to find the truth. "Fake news" with an innocent motive, if you like.

This takes us to an important question. Does misinformation in general link to foreign interference? You might think, yes it must. It is certainly true that foreign states or their proxies might circulate misinformation in the course of an influence campaign targeting Canada or Canadian interests. But misinformation would generally not involve the key elements of clandestinity, or deception, or threats of violence, which are important to our understanding of what constitutes foreign interference.

1 Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions (hereafter PIFI) , "Definitions of Key Terms in the Commission's Terms of Reference," Overview Report COM0000331, https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Exhibits_and_Presentations/Presentations/1_-_Key_Terms_and_Definitions_Definitions_de_termes_cles.pdf

2 ibid

3 Canadian Centre for Cyber Security, "How to Identify misinformation, disinformation and malinformation," https://www.cyber.gc.ca/sites/default/files/misinformation-mesinformation-itsap.00.300-en.pdf

4 ibid

So, the circulation of misinformation does not constitute foreign interference.

Where we do find these elements is in another branch of false information—**disinformation**.

The CCCS guide defines disinformation as:

"false information that is intended to manipulate, cause damage, or guide people, organizations, and countries in the wrong direction." [5]

The key here is malicious intent. The link to foreign interference is when state actors or their proxies get involved in sponsoring disinformation and, remembering our definition, do so either clandestinely or deceptively. That is, they try to hide the fact that their hand is behind such information operations. The "innocence" of fake news, which we can find in most forms of misinformation is gone.

What about the third branch of MDM—"malinformation." This term is probably least familiar to Canadians. The definition offered by the Cyber Centre is:

"information that stems from the truth but is often exaggerated in a way that misleads and causes potential harm." [6]

Malinformation exists on the borderline between misinformation and disinformation. It's a slippery term and can only really be pinned down in the context of actual usage. Its most dangerous manifestation is when malinformation is aligned with disinformation campaigns, notably in the deliberate use of automated bots to amplify messages. In such circumstances, malinformation becomes a technologically boosted form of disinformation.

We need to appreciate the various forms that" fake news" can take in our information ecosystem. But out of the complexity of the phenomenon emerges one, overriding phenomenon—namely that disinformation poses the greatest threat to open, truthful discourse. Why? Because it has a strategic purpose at heart and has the power and capabilities of a foreign adversary state or proxy behind it. Disinformation is a part of the foreign interference toolbox—as we have defined foreign interference--in ways that misinformation and even malinformation are not.

Transnational repression is a widely used term. But as the final report of the Foreign Interference Commission relates, there is currently no legal definition to draw on. The common understanding among Canadian government agencies is that transnational repression involves foreign state activity to monitor, intimidate and harass diaspora communities to achieve foreign state objectives.[7] A less bloodless definition is provided by the NGO, Freedom House:

"It is governments reaching across borders to silence dissent among diasporas and exiles, including through assassinations, illegal deportations, abductions, digital threats, Interpol abuse, and family intimidation." [8]

A special branch of transnational repression involves online campaigns—this is called "Digital Transnational Repression." As a Citizen Lab report from the University of Toronto notes:

"While transnational repression is not a new phenomenon, such practices are expanding through the market growth of digital technologies and the spread of Internet connectivity, among other factors. This digital dimension of transnational repression—which we refer to as digital transnational repression—is rapidly becoming the cornerstone of everyday transnational repression and is a threat to the rights and freedoms of dissidents and activists who are living in exile."[9]

5 ibid

6 ibid

7 PIFI, Final Report, Volume 1, p. 99

8 Freedom House, "Transnational Repression," https://freedomhouse.org/report/transnational-repression#:~:text=What%20is%20Transnational%20Repression%3F,Interpol%20abuse%2C%20and%20family%20intimidation.

9 Noura Al-Jizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert. «Psychological and Emotional War: Digital Transnational Repression in Canada,» Citizen Lab Research Report No. 151, University of Toronto, March 2022, https://utoronto.scholaris.ca/server/api/core/bitstreams/84d7937d-3383-48e7-9b0d-51ba9a70b4ef/content

FOCUS ON FOREIGN INTERFERENCE

If media stories launched public awareness of foreign interference threats, Canadians now have an opportunity to learn much more about these threats through the reporting of official investigative and review bodies.

This guide attempts to summarize for a public audience some key findings from this work, including the May 2023 report of the Independent Special Rapporteur; the June 2024 report of the National Security and Intelligence Committee of Parliamentarians; and the final report of the Public Inquiry into Foreign Interference, published on January 28, 2025. The Public Inquiry final report stands at the pinnacle of all these studies, notably for the connections it draws between foreign interference, disinformation, and transnational repression.

The Government of Canada announced the appointment of an Independent Special Rapporteur in March 2023 to investigate foreign interference targeting Canadian elections. The Honourable David Johnston, a former Governor General of Canada was named to the position and given terms of reference to study the impact of foreign interfere in Canada's electoral processes and review the Government's response to the threat. He worked quickly and issued his first report on May 23, 2023. The conclusions he reached can be summarized as follows:

- *Foreign interference is a "growing threat to our democratic system."*
- *The government's capacity to deal with the threat needed to be strengthened, particularly in the effective use of intelligence.*
- *Media reporting on foreign interference was sometimes exaggerated or taken out of context.*
- *Public hearings needed to be held to further a public debate and heighten awareness of foreign interference.* [10]

The last point was noteworthy, especially because David Johnston indicated that in the next phase of his study he wanted to "hear from Canadians," especially from diaspora communities and individuals who had experienced foreign interference.[11] He appreciated that foreign interference impacted significantly on Canadian diaspora communities, especially as a form of transnational repression.

The potentially important effort to "hear from Canadians," planned for the summer of 2023, never came to pass, as the ISR's rejection of a formal judicial process for investigating foreign interference roused the ire of opposition political parties and caused them to reject his report. Mr. Johnston resigned as ISR on June 9, 2023. His letter to the Prime Minister stated that his objective had been to "help build trust in our democratic institutions." He went on to say, "I have concluded that, given the highly partisan atmosphere around my appointment and work, my leadership has had the opposite effect."[12] Opposition party spokespersons said Johnston had done the right thing in resigning and blamed the government for putting him in an impossible position by refusing to endorse a public inquiry in the first place. They did not, of course, blame themselves for besmirching Johnston's reputation. [13]

The flame-out of the Independent Special Rapporteur process left the government, in a minority situation in Parliament, with no option but to accede to opposition political party demands for a judicial inquiry. The key remaining question involved the scope of any planned public inquiry to be headed by a judge. Terms of reference were hashed out in closed-door meetings between the government and representatives of the opposition parties over the summer of 2023. By September, the process was

10 First Report, The Right Honourable David Johnston, Independent Special Rapporteur on Foreign Interference, May 23, 2023, p.1, https://www.canada.ca/en/democratic-institutions/services/reports/first-report-david-johnston-independent-special-rapporteur-foreign-interference.html

11 Ibid, "Issues for Review in the Public Stage of my work," pp. 54-55

12 Letter, David Johnston to Prime Minister Trudeau, June 9, 2023, https://s3.documentcloud.org/documents/23840359/resignation-letter-to-the-rt-hon-justin-trudeau-from-the-rt-hon-david-johnston.pdf

13 CBC, "David Johnston resigning as special rapporteur on foreign interference," June 9, 2023, https://www.cbc.ca/news/politics/david-johnston-resigns-1.6871761

ready to be launched with the agreed appointment of a Quebec Superior Court judge, Marie-Josee Hogue, to head the inquiry, and agreed terms of reference.

It was a landmark moment in a public approach to understanding the threat of foreign interference and all that it entails.

THE PUBLIC INQUIRY INTO FOREIGN INTERFERENCE (PIFI)

Rehearsing this history is important to understanding what the Public Inquiry was meant to do, and what limits were placed on it. To see this clearly, we need to briefly explore the Inquiry's terms of reference. [14]

The key elements of the terms of reference involved its short time-frame, with a final report initially mandated for December 2024; the open-ended scope of the foreign interference actors it could examine (China, Russia and any other foreign states or non-state actors); the need to look back and examine past foreign interference campaigns against the 2019 and 2021 federal elections; and the requirement to look ahead and make recommendations to better protect "federal democratic processes."

Two things are especially worthy of note regarding the Inquiry's mandate. One is that there was no explicit mention of disinformation as a vector of foreign interference. The other is that the Inquiry was specifically directed to examine the Government' capacity to respond to foreign interference in relation to:

"the supports and protections in place for members of a diaspora who may be especially vulnerable and may be the first victims of foreign interference in Canada's democratic processes." [15]

This clause seemingly gave a green light to the Public Inquiry to link foreign interference in Canada's elections to the broader themes of transnational repression. Its efforts in that regard failed to satisfy critics, especially from diaspora groups, as we shall see.

The Public Inquiry: Foreign interference and its connections to transnational repression and disinformation

The Inquiry's final report was published on January 28, 2025. It involved seven volumes and made 51 recommendations. All Canadians should be encouraged to familiarise themselves with Volume 1 of the final report, the "Report Summary." This volume provides the overview of the Commission's findings and its recommendations.

There are many takeaways from the PIFI final report. Not all will be covered in this guide. Here, I will zero in on what recommendations were made about protecting diaspora communities against the phenomenon known as transnational repression (often abbreviated as TNR) and what we might learn about the disinformation threat.

Disinformation is worthy of attention not least because it was not considered central to the initial terms of reference but emerged over the course of the Commission's work as a major threat, especially for the future. The threat to diaspora communities from transnational repression was recognised, as we saw, in the initial terms of reference, so the question becomes: how, and how well, did the Inquiry respond to it? As we shall see, threats to diaspora communities and disinformation campaigns lock together.

14 PIFI, "Terms of Reference," https://www.canada.ca/en/democratic-institutions/general/terms-reference.html

15 Terms of Reference, clause "C," "ii"

THE PUBLIC INQUIRY AND TRANSNATIONAL REPRESSION

The Inquiry found itself facing a dilemma when it came to an investigation of transnational repression. On the one hand, Justice Hogue recognised the threat posed by transnational repression. On the other hand, the Justice reached the conclusion that her terms of reference, provided to her by the government with the agreement of opposition political parties, focused on foreign interference and impacts on elections, and precluded an in-depth examination of transnational repression.

Here is what was said, candidly, on this point in the PIFI final report:

"My terms of reference did not allow for an in-depth study of transnational repression in Canada. Thus the work that the Commission did in this respect likely only scratched the surface of this phenomenon. What this work has made clear to me, however, is how serious a problem transnational repression is, how harmful its impacts are on individuals, and how important it is for the government to meaningfully respond to it." [16]

It is, however, clear that the Commissioner was deeply affected by what she had learned through the process of public consultations about the impacts on people affected by transnational repression. The volume of information provided to the Commission through these consultations is too great to treat here, but the Commissioner's own summary is a good indication.

Justice Hogue stated that a "substantial proportion of the incidents can be qualified as very severe and shocking."[17] The many threats she heard about included threats of physical violence, sexual violence and even "threats to life." Members of diaspora communities spoke of family members being used as leverage to prevent expressions of dissent, and of harassment and efforts at exclusion experienced within their own communities. People feared being the subject of surveillance. Some spoke of having consular services denied to them. [18]

Fear, chilling effects on free speech and community activity, and the undermining of a sense of belonging to Canadian society—these were some of the grave impacts reported to the Commission.

The experiences of diaspora members who reported experiencing transnational repression from Eritrea and Ethiopia, India, Iran, the People's Republic of China (including Uyghurs, Falun Gong practitioners, Tibetans), Russia, and Sri Lanka all featured in the Public Inquiry's work. [19]

As we have seen, the Inquiry's terms of reference required it to consider:

"the supports and protections in place for members of a diaspora who may be especially vulnerable and may be the first victims of foreign interference in Canada's democratic processes." [20]

What, then, did the 16-month long investigation of foreign interference have to say about these "supports and protections" given what the Commission had heard through its public consultations?

The PIFI final report itemised 7 measures to provide such supports and protections against TNR.[21]

One involved the efforts of Heritage Canada, though its "Digital Citizen Initiative," to fund projects to help understand transnational repression. Two involved diplomatic efforts to address transnational repression with allies and adversaries. Another involved the work of Elections Canada to publish voting guides (available in 51 languages) and to engage with diaspora communities.

16 PIFI, Final Report, Volume 1, p. 101

17 PIFI, Final Report, Volume 6, p. 20

18 Ibid, pp. 21-22

19 Ibid, pp. 22-29

20 PIFI, Terms of Reference, clause "C," "ii"

21 PIFI, Final Report, p. 99

The remaining three measures spoke more directly to domestic security protections. They include:

- *The work of the National Counter Foreign Interference Coordinator;*
- *A CSIS hotline;*
- *CSE cyber operations.*

It's not a long list. Let's look at these in turn.

The National Counter Foreign Interference Coordinator (NCFIC).

This is a recently created position in the federal government and likely to be little known to Canadians. Its newness and low profile are not helped by the fact that there is minimal public information provided about the Coordinator and there is no dedicated website or web pages for their work. Public Safety Canada provides a one-line description on its website pages devoted to "Foreign Interference and Canada."[22] The update provided by the Clerk of the Privy Council and Minister LeBlanc in April 2023, "Countering an Evolving Threat," mentions the role of the NCFIC, again very briefly, saying:

"the Government will use the New National Counter Foreign Interference Coordinator and CSIS's upcoming annual report to bolster communications with Canadians." [23]

In its submission to the PIFI, the Centre for International Governance tried to expand on this promise by urging that "the new office of the National Counter Foreign Interference Coordinator be strengthened, provided with additional resources, be full connected to intelligence reporting and develop a coherent strategic plan for public outreach, education and parliamentary engagement." [24] Unfortunately, the PIFI Final report offers no recommendations regarding the work of the NCFIC. It merely suggests that the role is still new and remains a "work in progress."[25] It offers the observation that the NCFIC "is bringing a transnational repressions action plan to the Deputy Minister of Public Safety."[26]

Given the potential significance of the role of the NCFIC in responding to FI and acting as a source of engagement with diaspora communities, the failure to explore the NCFIC function more fully and make recommendations amounts to an important missed opportunity.

The CSIS "hotline" for anonymous reporting on foreign interference listed by PIFI as a key measure to counter FI is, in fact, one of many. This may cause confusion and pose problems for any coordinated response. Guidance offered by Public Safety Canada on its website indicates that people may contact the RCMP "to report suspicious incidents which may be of concern to national security." Alternatively, they may contact CSIS "to report non-urgent potential national security threats or suspicious activities," though how one would determine whether to contact the RCMP or CSIS is not made clear. For cyber threats, Canadians are encouraged to contact the Canadian Centre for Cyber Security. For "non-urgent suspicious cross-border activities, contact the Canada Border Services Agency. To report a "threat or immediate danger," call 9-1-1 or "contact local police." [27] There is no mention of reporting disinformation and the language of "national security" is far too generic.

The CSIS guidance on its website distinguishes between an "immediate" threat (left undefined) to national security, in which case people are advised to phone 911 or contact local law enforcement, and a "non-immediate" threat to national security where they can phone CSIS or fill out a web page. [28]

22 Public Safety, "Foreign Interference and Canada," https://www.canada.ca/en/public-safety-canada/news/2024/05/foreign-interference-and-canada.html

23 Government of Canada, "Countering an Evolving Threat: Update on recommendations to counter foreign interference in Canada's democratic institutions," March 2023, https://www.canada.ca/en/democratic-institutions/services/reports/countering-evolving-threat.html

24 Centre for International Governance Innovations, Submission to the Public Inquiry, https://www.cigionline.org/publications/final-submission-to-the-public-inquiry-into-foreign-interference-in-federal-electoral-processes-and-democratic-institutions-in-canada/

25 PIFI final report, volume 1, p. 53.

26 Government of Canada, "Countering an Evolving Threat: Update on Recommendations to Counter Foreign Interference in Canada's Democratic Institutions," April 2023, https://www.canada.ca/content/dam/di-id/documents/rpt/rapporteur/Countering-an-Evolving-Threat.pdf

27 Public Safety Canada, "How to report foreign interference." https://www.publicsafety.gc.ca/cnt/ntnl-scrt/frgn-ntrfrnc/hr-en.aspx

28 Canadian Security Intelligence Service, "Reporting national security information." https://www.canada.ca/en/security-intelligence-service/corporate/reporting-national-security-information.html

This hodgepodge is less than helpful. The PIFI recognised this by advancing a recommendation for an improved and centralised hotline. In the words of the Final Report:

"There should be a single, highly visible and easily accessible point of contact or hotline for reporting foreign interference to the government, which is responsible for engaging the appropriate agency or department." [29]

The Final Report also addressed the frustration it had heard from diaspora community members, and even MPs, about government agency response. It recommended that:

"Follow up with those who seek support should be systematic and ensure that those who make reports fully understand what can and cannot be done in response." [30]

What the Commission was clearly alluding to was that for any hotline to be effective, its existence had to be known, understood, and trusted by potential users. There also had to be appropriate resources and understanding at the receiving end. Other recommendations reflected this concern, including one that emphasises that "intelligence agencies should continue to diversify their personnel based on cultural, ethnic and linguistic background," (Recommendation 18). [31]

In addition to its hotline, CSIS has a small unit called the "Academic Outreach and Stakeholder Engagement (AOSE)." The unit was originally established in 2008 and revised in its scope in 2019. The work of this unit, and more broadly CSIS public engagement efforts, are chronicled briefly in CSIS's most recent annual public report, for 2023, published in May 2024.[32] It notes that CSIS conducted 147 outreach engagements in 2023. While that number sounds impressive, a breakdown of the sectors involved shows that only 7% of these engagements involved "community groups." There is no category for engagement with diaspora communities. [33]

The most relevant of the publications produced by CSIS AOSE is a small pamphlet entitled "Foreign Interference and you." [34] It is 5 pages in length and offers brief and high-level descriptions of the nature and aims of foreign interference; the national security threat involved; Canada as a "permissive target;" the sectors of Canadian society that may be in the crosshairs of foreign interference, especially academia and research; and some common techniques. The document reflects the fact that CSIS continues to be invested in and believe that "traditional interference through human intelligence operations remains the greatest danger." [35]

The CSIS program has also created an external newsletter called "Need to Know." It is web based and sent out via email to selected individuals. How wide an audience it reaches is not known to me. An issue published on March 23, 2023, was jointly edited with the Chinese-Canadian National Council for Social Justice and discussed foreign interference.

The CSIS AOSE pamphlet on foreign interference does offer some advice to individuals and organizations. These mostly put the onus on the targets of foreign interference. The first bullet addressed at individuals says: "Be aware of the threat; increasing our collective resilience against foreign interference is a shared responsibility." [36]

Collective resilience was also one of the messages of a public threat assessment that CSIS produced in July 2021, on "Foreign Interference Threats to Canada's Democratic Process."[37] It noted that FI targets what it referred to as "diverse Canadian communities" seeking to manipulate and suppress opinion

29 PIFI, Final Report, Recommendation 17, Volume 1, p. 114

30 ibid

31 Ibid, p. 115

32 Canadian Security Intelligence Service Annual Public Report, 2023, published May 2024, https://www.canada.ca/content/dam/csis-scrs/documents/publications/Public_Report_2023-eng-DIGITAL.pdf

33 Ibid, p. 62

34CSIS, "Foreign Interference and You," https://www.canada.ca/content/dam/csis-scrs/documents/publications/2021/foreign-interference-and-you/AOSE_ForeignInterferenceHandout%20-%20Digital_ISBN_A.pdf

35 Ibid, p. 2

36 Ibid, p. 5

37 Canadian Security Intelligence Service, "Foreign Threats to Canada's Democratic Processes," July 2021, https://www.canada.ca/content/dam/csis-scrs/documents/publications/2021/foreign-interference-threats-to-canada%27s-democratic-process.pdf

through the use of fear tactics. CSIS also observed that foreign interference efforts were increasingly moving online, especially through intrusions into social media. [38]

The CSIS threat assessment also listed and described a variety of techniques used by state actors to perpetrate foreign interference, including disinformation campaigns. Each technique was accompanied by a short statement about how individual and organization could respond. For disinformation, three pieces of advice were offered:

- *Be critical of what you consume online*
- *Be careful about sharing of in formation online*
- *Take note of "unexpected" online interactions* [39]

The CSIS paper ends with hotline contact information for the Service and for the RCMP. [40]

It is not clear from the description how a concerned Canadian might choose between reporting something to CSIS or to the RCMP.

The CSIS threat assessment paper has not been updated in public since July 2021. It does not use the terms "diaspora" or "transnational repression." Its advice to Canadians on responses is, like the AOSE paper, generic and high-level with an onus on individual responsibility to act.

Direct mention of the RCMP's role in providing supports and protections for those facing transnational repression is strangely absent from the PIFI Final report, despite the fact that the Commissioner heard from representatives of diaspora groups that their members' experience in reporting incidents to the RCMP was deeply unsatisfactory. There is in the PIFI final report a small suite of recommendations aimed at the RCMP. The RCMP is urged to ensure that their officers working in affected communities receive appropriate training, including about transnational repression. Adequate resourcing of the RCMP is also considered important, as is recruitment, training and retention of staff with relevant skills for dealing with foreign interference. [41]

Of course, these recommendations suggest that all is not well when it comes to the ability of the RCMP to deal with foreign interference and engage in outreach with diaspora communities. The pity is that the Inquiry did not dig deeper into the RCMP's ability to conduct such engagement. The Mounties themselves offer no picture of their outreach strategy. Their website contains a page on "Foreign Actor Interference" which describes various types of FI, including "community intimidation and harassment," but offers no suggestions about how the Mounties and affected communities might work together, or what individuals or diaspora communities impacted by foreign interference might do about it.[42]

We learn a bit more about the RCMP's outreach activities from the "Institutional report" submitted to the PIFI and available on the PIFI website.[43] The document breaks down outreach and engagement activities into three categories: "tailored engagement with diaspora communities;" "cultural and educational initiatives;" and "responsive engagement." It then goes on to provide a list of activities according to the different RCMP Divisions across the country. Of the 48 activities listed, only 10 referenced outreach to diaspora communities, and of those 10 only 3, for example, appeared to be specific to the Chinese diaspora. The list does not provide any analysis of the effectiveness of these engagements or give any indication about any feedback the RCMP might have received. The majority of the engagements listed (20) involve the RCMP addressing a law enforcement audience. It is worth

38 Ibid., p. 8

39 Ibid, p. 13

40 Ibid, p. 15

41 PIFI Final Report, volume 1, Recommendations 36-38, p. 118

42 RCMP, "Foreign Actor Interference," https://rcmp.ca/en/federal-policing/national-security/foreign-actor-interference

43 RCMP Stage 2 Institutional Report, CAN.DOC.000042, https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Exhibits_and_Presentations/Exhibits/CAN.DOC.000042.pdf

noting that a similar listing provided to Justice Hogue by CSIS in its Institutional Report regarding CSIS AOSE engagement with diaspora communities is redacted (Table 4), in its entirety. [44]

This failure to enlarge on outreach activities by the agencies concerned is disappointing. It is even more disappointing that the PIFI did not assess the nature and current efficacy of these endeavours. Outreach is among the most important protective "measures" that national security agencies can apply to the problem of the impacts of transnational repression. It is at the heart of any solution to strengthen societal resilience. More, in future, needs to be said publicly about this by the key agencies concerned, the RCMP and CSIS, and more advocacy needs to be directed at outreach efforts by concerned diaspora groups.

There is an important role here for coordination and efficacy measurement that could be played by the NCFIC, with appropriate transparency to signal that attention is being paid.

CSE

Finally, among the seven measures listed by Justice Hogue, we can turn to the work of the the **Communications Security Establishment (CSE)**. CSE is Canada's foreign signals intelligence and cyber security agency. The CSE Act passed in 2019 expanded its mandate to include five roles: [45]

- *Foreign signals intelligence*
- *Cyber security (or "assurance")*
- *Active cyber operations*
- *Defensive cyber operations*
- *Assistance to other federal law enforcement and security agencies.*

The meaning behind the reference in the PIFI final report unclear. It simply states that "some of its cyber operations have repercussions for transnational repression."[46] Repercussions could be a reference to CSE's authorities to engage in cyber operations against foreign targets to pre-empt cyber-attacks. But if we are looking for ways that CSE can directly assist individuals and communities affected by foreign interference, we turn to the entity created by CSE in 2018 called the Canadian Centre for Cyber Security (CCCS). The CCCS offers on its website public information and guidance on cyber threats.[47] Included is a campaign called "Get Cyber Safe," with various advisories on securing computer systems and personal devices. [48] The CCCS website does not feature targeted advice for diaspora communities or those facing transnational repression. The website material is only available in English and French.

However, CSE does publish both a regular series of public reports on cyber threats to Canada's democratic processes as well as a more general cyber threat assessment, issued as a bi-annual product.

The most recent version of the "Cyber Threat to Canada's Democratic processes" is a 2023 Update.[49] It identified four major trends including that the use of cyber-attacks against national elections is on the rise worldwide; and that Russia and China are the main threat actors. The report also found, worryingly, that much of the cyber activity directed at electoral processes is unattributed. This is thanks to the such cloaking techniques as the increased use of non-state cyber groups as proxies and the availability of a new industry of 'cyber-crime for-hire firms.' Finally, the CSE threat assessment found that the use of

44 CSIS Institutional Report, PIFI database, CAN.DOC.000044, https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Exhibits_and_Presentations/Exhibits/CAN.DOC.000044.pdf

45 Communication Security Establishment Act, 2019, https://laws-lois.justice.gc.ca/PDF/C-35.3.pdf

46 PIFI, Final report, vol. 1, p. 99

47 Canadian Centre for Cyber Security (CCCS), https://www.cyber.gc.ca/en

48 CCCS, "Get Cyber Safe," https://www.getcybersafe.gc.ca/en

49 CSE, "Cyber Threats to Canada's Democratic Processes, 2023 Update," https://www.cyber.gc.ca/sites/default/files/cyber-threats-canada-democratic-process-2023-update-v1-e.pdf

generative AI to sponsor synthetic content ("deep fakes"), and its incorporation in proliferating botnet networks able to spread MISDISMAL is also on the rise.

These findings were placed in a broader strategic context in the national threat assessment series published by the Canadian Centre for Cyber Security (CCCS). The most recent in this bi-annual series cover the years 2024-2025.[50] The CCCS assessment tracks both state actor threats and those posed by criminal organizations; identifying state actors as posing strategic threats to Canadian governance and organized crime being the most serious threat to ordinary Canadians and businesses, especially through ransomware attacks.

State actors, including the PRC, Russia, Iran are of concern for espionage campaigns and critical infrastructure reconnaissance and penetrations, but are also noted to engage in cyber operations for transnational repression purposes.

The PRC is identified as posing the top cyber threat to Canada. The threat assessment finds it "very likely" that PRC cyber threat actors support Chinese efforts to target advocates for groups the regime views as security threats, the co-called "Five Poisons."[51] This group includes Falun Gong practitioners; advocates for the rights of Uyghurs and Tibetans; supporters of Taiwanese independence; and pro-democracy advocates. According to the CCCS threat assessment:

- *"PRC actors very likely facilitate transnational repression by monitoring and harassing these groups online and tracking them using cyber surveillance."* [52]
- *It notes a particular case involving the targeting of members of the Uyghur diaspora in Canada in a campaign involving spear phishing emails and spyware.*
- *The report also indicates that the PRC "leverages" Chinese -owned technology platforms to facilitate transnational repression.*[53] *It does not name any specific platforms.*

The Russian cyber program is described as "unpredictable." Russia is believed to "combine conventional cyber espionage and computer network attacks with disinformation and influence operations."[54] The Russian threat stands apart, according to the CCCS, for its reliance on a hybrid strategy using many different kinds of proxies, whose motives ranging from patriotism to criminal profit to sheer opportunism, in an effort to ensure 'plausible deniability.' [55]

The Islamic Republic of Iran is characterized in the CCCS threat assessment as a state that uses cyber-attacks, around the world, "to intimidate Iran's opponents, signal the regime's displeasure and persuade a country to change its behaviour."[56] Canada is not seen as a priority target of Iran's cyber aggression, but the CCS report notes that that could change depending on the degree of tension in future Iranian Canadian relations.

Of the two other state actors noted in the threat assessment, the cyber campaigns mounted by the Democratic People's Republic of Korea (DPRK) are found to be mostly grounded in efforts at financial gain[57] India's cyber program is depicted as in the course of "modernization" and that future operations targeting Canada will depend on the state of relations between the two countries. [58]

50 CSE/Canadian Centre for Cyber Security, National Cyber Security Threat Assessment 2024-2025, https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf

51 bid, p. 12

52 ibid

53 ibid

54 Ibid, p. 14

55 Ibid

56 Ibid, pp. 16-17

57 Ibid, p. 18

58 ibid

The global picture of state cyber threat actors presented by the Canadian Centre for Cyber Security makes very clear that some are using cyber capabilities, both state-based and through proxies, to engage in transnational repression, including through disinformation campaigns. As valuable as this assessment is, the TNR threat is embedded in a lot of other information about other forms of cyber threats both from state and non-state actors. The Communications Security Establishment's mandate is to protect government information systems and designated systems controlled by the private sector. It is not to protect ordinary Canadians, except through these efforts. It can only offer general cyber hygiene guidance. [59]

We turn now to a different official report on foreign interference, that published by the National Security and Intelligence Committee of Parliamentarians (NSICOP) in June 2024. [60] Two things are noteworthy about the Committee's report at the outset. One is that it focused, as did its previous 2019 study, on what it terms "traditional" foreign interference, conducted through person-to-person interactions. The Committee continues to believe that these tradition forms of FI predominate, which means that it pays relatively little attention to newer, "non-traditional" efforts, including through disinformation operations. The Committee also took an approach similar to that of the Public Inquiry in that it identified the "most egregious" threat of transnational repression as a vector of foreign interference but did not consider it a focus for its review. Instead, it contented itself with saying:

"The Committee condemns this [a reference to the Hardeep Singh Nijjar assassination] and all instances of transnational repression and considers them a threat to Canadian values, human rights and democratic freedoms." [61]

NSICOP, a body consisting of appointed Parliamentarians, chose to focus instead on the FI threat to Parliamentarians and made some sensational allegations about members of Parliament being witting or semi-witting accomplices of foreign interference schemes. These allegations were essentially dismissed in the PIFI final report. None of the recommendations advanced by NSICOP involved responses to transnational repression or disinformation campaigns, though it did draw attention to failures of transparency on the part of the government. [62]

OFFICIAL REPORTS AND THE THREAT POSED BY TNR

As has been demonstrated, there is plentiful material in multiple official government reports that touch on the threats of foreign interference and transnational repression, including in CSIS and CSE public reports. The trouble lies in the fact that there are so many different reports, most of which depend on the public's ability to find them and understand their perspective. This is where the PIFI final report should have come in.

The Public Inquiry into Foreign Interference stands at the pinnacle of this public reporting. The PIFI might reasonably have been expected to draw the existing documentation together in a comprehensive way and at least paint a picture of the range of transnational repression involved in foreign interference. It largely failed to do so. [63]

Instead, in its overview volume, the Inquiry restricted itself to two, well-known examples. One was the so-called "Chinese police stations." The PIFI final report noted that responding to the PRC overseas police stations on Canadian soil was a complicated matter, as they could perform both legitimate administrative functions for the local Chinese community as well as be a nexus for transnational repression activities by PRC officials under that very same guise. Typically, PRC "police stations" were run by Canadian citizens. When the RCMP used visible disruption tactics to deal with the threat, the Inquiry noted that they met with a range of responses from diaspora community members, from criticism of the RCMP actions as damaging to the community, to a view that the actions taken were

59 Ibid, "Conclusion," p. 38

60 National Security and Intelligence Committee of Parliamentarians, (NSICOP "Special Report on Foreign Interference in Canada's Democratic Processes and Institutions," June 2024, https://nsicop-cpsnr.ca/reports/rp-2024-06-03/special-report-foreign-interference.pdf

61 Ibid, p. 61

62 Ibid, "Recommendations," p. 75

63 Here I focus on the material presented in volume one, the overview report, of the PIFI. There is additional chapter on TNR in Volume 4 (chapter 17) of the Final report which offers some elaboration.

not strong enough.[64] The NSICOP also drew on the example of PRC stations in its brief discussion of transnational repression. [65]

The second example of transnational repression briefly documented in the PIFI final report overview involved the assassination of a Canadian Sikh activist, Hardeep Singh Nijjar on June 18, 2023. The Inquiry documented the evolution of the case after intelligence emerged about India's involvement in the summer of 2023 and reached another dramatic high point with an RCMP press conference in October 2024. The outline of the Nijjar assassination made no mention of its impact on the Canadian Sikh or South Asian communities, contenting itself with a note that: "any effective response to foreign interference must consider the realities of transnational repression in Canada." [66]

Justice Hogue concludes about the measures to support those targeted by foreign interference:

"The government must continue to involve individuals, groups and communities in a whole-of-society approach to addressing foreign interference, especially transnational repression. Facilitating the involvement of individuals and groups, including those directly impacted, will be crucial to Canada's ongoing efforts to detect, deter and counter foreign interference." [67]

The government, she says, "needs to ramp up its efforts." [68] Justice Hogue offers no specific recommendations in that regard.

In the aftermath of the final report, the public inquiry has been criticised as a missed opportunity to deepen Canadians' understanding and recommend concrete measures for a stronger governmental response.[69] Even taking into account the limitations of the Inquiry's mandate, these criticisms are valid. An Opinion column in the Globe and Mail reiterated the call of advocacy groups to treat transnational repression as a distinct form of foreign interference that requires tailored responses.[70] As we have seen, transnational repression can become submerged in broader outlooks and policies on foreign interference. Too often even literal references to diaspora communities and to transnational repression are missing.

But in terms of one technique of transnational repression, that involving digital disinformation operations, the Inquiry did important service in at least calling attention to the problem.

THE DISINFORMATION THREAT

Disinformation campaigns are structured information operations conducted by a foreign state actor and/or their proxies in an effort to manipulate the information environment of a target state or population. They are conducted clandestinely and deceptively and involve the deliberate circulation of fake news and falsehoods. The element of clandestinity is important because it involves an effort to cloak the origins of such campaigns and heighten their impact on a target information space. Digital disinformation campaigns operate with the benefit of access to a proliferating universe of social media platforms, some of which can be state-influenced and many of which have few to no controls on content. Online disinformation campaigns also can be weaponized through the availability of technological tools, including generative AI ,and automated amplification of circulation through botnets.

64 PIFI final report, Vol. 1, pp. 99-100

65 NSICOP special report, pp. 13-14

66 PIFI final report, Vol. 1, pp. 100-101

67 Ibid, p. 106

68 Ibid, p. 110.

69 Robert Fife and Steve Chase, "Diaspora groups criticize Justice Hogue report on Foreign Interference," January 29, 2025, The Globe and Mail, https://www.theglobeandmail.com/politics/article-diaspora-groups-criticize-justice-hogue-report-on-foreign-interference/;

70 Ron Deibert et al, "The Final report of the Hogue Inquiry was a missed opportunity to tackle transnational repression," The Globe and Mail, February 10, 1025, https://www.theglobeandmail.com/opinion/article-the-final-hogue-report-was-a-missed-opportunity-to-tackle/

While state resources and technological tools give disinformation a threatening edge, we also need to consider the context of such information operations.

In many cases, disinformation operations are conducted by authoritarian states with significant domestic surveillance and censorship capabilities, against target democracies. They bring their domestic cultural norms and practices with them in the conduct of such overseas operations. But to be able to have an impact disinformation needs more than brute force, it needs a sophisticated understanding of its target. That can be challenging in the circumstances of authoritarian state operations against democracies. Between such political systems, there can be a significant understanding divide.

The second element at play in disinformation operations is that an adversary state has to be able to identify a malleable information environment with a particular focus on a segment of a population, often on a diaspora community. A foreign state conducting or facilitating a disinformation campaign has to believe that there is a population segment or a diaspora community it can target because it will be listened to, and its messages maybe accepted. Where a foreign state controls or influences some platforms for information operations this can become part of a perceived recipe for success. Where a foreign state believes diaspora communities owe it loyalty, including because of family members who remain in the country of origin, this can be an additional element of the playbook.

Imagining and delivering disinformation operations depend on both elements, sophisticated understanding of a target audience and access to that audience. This is because disinformation operations rarely succeed by trying to generate entirely new ideas. They instead work to bolster, skew, amplify existing concepts. The formula is an old one—the best propaganda works by convincing consumers of what they already (at least partly) believe. A RAND report from 2016 remains very relevant to disinformation operation models in place today. It emphasises the importance of volume, multiple channels of delivery, creating 'first impressions' and articulating something seemingly familiar, as key contributors to establishing credibility. [71]

The very strengths of disinformation operations—state resources and intent; the weaponization of technology; targeted access may also, paradoxically, be elements of weakness, in part because they point to counter-measures. [72]

WHAT THE PIFI SAID

In a nod to the June 2024 NSICOP report discussed above, the final report of the Foreign Interference Inquiry recognized the significance of traditional (human-to-human) forms of foreign interference but argued that a new reality had emerged, namely that "misinformation and disinformation pose an even greater threat to democracy."[73] Justice Hogue went on to say, in what might be the most striking phrase in the entire report:

"In my view it is no exaggeration to say that at this juncture, information manipulation (whether foreign or not) poses the single biggest risk to our democracy. It is an existential threat." [74]

Three cautions must, however, be raised about this striking statement. The first is that the Commissioner should not have lumped foreign-directed disinformation campaigns and domestic misinformation together as one unified threat. They must be distinguished, as noted earlier in this report. A second is that no analysis is offered to support the idea that "information manipulation" amounts to an existential threat. It is not even clear what the Commissioner means by "existential" a word that must be used carefully, especially in the context of reporting based on intelligence. A third note is that the PIFI fails to deliver any real discussion of the nature of "information manipulation."

71 RAND Insight report, "The Russian 'Firehose of Falsehood' Propaganda Model,' July 11, 2016, https://www.rand.org/pubs/perspectives/PE198.html

72 Wesley Wark, "Disinformation is a Pickpocket nothing more: It shouldn't shake us," Centre for International Governance Innovation (CIGI), July 6, 2023, https://www.cigionline.org/articles/disinformation-is-a-pickpocket-nothing-more-it-shouldnt-shake-us/

73 PIFI final report, vol. 1, p. 5

74 Ibid, p. 6

The PIFI final report is instead limited to some general observations about concerns that "foreign state influence over media can be a powerful tool for foreign interference." The report states that:

"foreign threat actors manipulate both social and traditional media to spread disinformation, amplify a particular message or provoke users. People unaware of the origins of the content or the intent of the threat actor may unintentionally spread disinformation to others. This is misinformation." [75]

I would not agree with this blurring of distinctions. The circulation of disinformation remains disinformation—it is an intended consequence of the strategy.

The only place to look for more on the subject of disinformation, is to turn to the PIFI set of recommendations offered at the close of the Overview volume of the final report. Even here, the recommendations are not bunched together.

There are two distinct sections of the recommendations. One, important and indeed bold, involves the creation of an open-source intelligence "entity" within the federal government structure. The Commissioner of course recognizes that any such entity must be rooted in law and respectful of Charter rights. The report defines the purpose of the "entity" as being to: "monitor the domestic open source information environment for misinformation and disinformation that could impact on Canadian democratic processes."[76]

Again, we see this unfortunate mashing together of disinformation and misinformation. Misinformation is organic to any democratic discourse and, in my view, there is no place for the government to be involved in its targeted monitoring. Disinformation is a deliberately weaponized form of information manipulation planned and directed by a foreign state adversary to achieve a specific objective. As an adversary weapon, of potential consequence to democratic processes, it must be monitored. But to what end? I will come back to this in the discussion on attribution.

The second set of recommendations advanced by Commissioner Hogue are discussed under two sequential themes: "navigating the information environment" and "developing digital and media literacy." There are five recommendations included under these two themes. They include exploring options for media funding, including for local and foreign language media, expanding the use of AI translation tools, funding educational programs on media use for new Canadians, requiring the labelling of "altered content," a reference to "deep fakes," by media platforms; and development of some kind of publicly available tool "to help citizens verify whether digital content is fabricated or altered."[77] This last recommendation presumably reflects a concern that regulations for labelling altered content may be ineffective. But it is very unclear how realistic the development of such a tool, in the face of fast-paced technological change, might actually be, or how it would be offered to Canadians.

Other than question marks surrounding regulation of deep fakes or the creation of identification tools, these are all good and sensible ideas which deserve implementation.

What they are not are sufficient responses to disinformation.

75 Ibid, volume 3, p. 15

76 Ibid, volume 1, Recommendations #10 and 11, p. 113

77 Ibid, Recommendations #44-46; and #47-48, p. 120

THE IMPORTANCE OF ATTRIBUTION OF DISINFORMATION CAMPAIGNS

If the government has a responsibility to "detect, deter and counter" foreign interference, that responsibility must be extended to dealing with digital FI and to the very real prospect that digital foreign interference will be used as a tool of transnational repression.

Dealing with disinformation is fundamentally, but not solely, a responsibility of government. Government national security and intelligence agencies possess unique tools to detect disinformation and to understand the strategic objectives that might be behind such campaigns.

Identifying disinformation campaigns is the first step. There are multiple agencies that can take a hand in such work, depending on their capacities and mandates, including CSIS, CSE, RCMP and Global Affairs Canada. What has been made abundantly clear in the government's intelligence priority setting exercise, now made public for the first time, is that foreign interference is a top-tier threat requiring an intelligence response. [78]

Fortunately, the government has developed some foundational capacities for detecting disinformation campaigns, based in the creation of the "Rapid Response Mechanism," that emerged out of Canadian-led G7 recommendations from the 2018 G7 leaders summit.[79] The RRM really first came to public attention during the Foreign Interference Inquiry because of its role as a member of the SITE (Security and Intelligence Threat to Elections) Task Force.

But detection without action is of little value. The next step is public "attribution." The RRM has emerged out of the shadows to make some announcements about disinformation campaigns. The most recent was a notice regarding a coordinated influence campaign mounted on the Chinese social media platform WeChat designed to target Liberal leadership contestant Chrystia Freeland. The announcement stated:

"RRM Canada detected coordinated and malicious activity about Ms. Freeland. The launch of this information operation was traced to WeChat's most popular news account – an anonymous blog that has been previously linked by experts at the China Digital Times to the People's Republic of China. RRM Canada identified over 30 WeChat news accounts taking part in the campaign. The campaign received very high levels of engagement and views, with WeChat news articles disparaging Ms. Freeland netting over 140,000 interactions between January 29 and February 3, 2025. RRM Canada estimates that 2 to 3 million WeChat users saw the campaign globally." [80]

Other notable RRM announcements, dating between August and October 2023, involved the detection of influence operations targeting Canadian Parliamentarians. [81]

The point of making these announcements is to move beyond detection to deterrence and countering effects. The deterrent element is, at least in theory, advanced by public statements designed to put perpetrators on notice that the Canadian government is watching and knowledgeable about specific campaigns. Countering effects depend on ensuring that the message of these RRM announcements reaches not just the specific targets of disinformation operations but a wider digital consumer marketplace.

Both deterrence and countering are relatively weak effects at present. There are a number of reasons for this, including the fact that the work of the RRM remains relatively unknown to a wider Canadian

78 Privy Council Office, "Canada's Intelligence Priorities," September 2024, https://www.canada.ca/en/privy-council/services/publications/canada-intelligence-priorities.html

79 For an overview of the work of the RRM, see Global Affairs Canada, "Rapid Response Mechanism," https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/index.aspx?lang=eng

80 Global Affairs Canada, "Rapid Response Mechanism detects information operation targeting a candidate for the leadership campaign of the Liberal Party of Canada," February 7, 2025, https://www.canada.ca/en/global-affairs/news/2025/02/rapid-response-mechanism-canada-detects-information-operation-targeting-a-candidate-for-the-leadership-campaign-of-the-liberal-party-of-canada.html

81 Global Affairs Canada, "Rapid Response Mechanism," "Latest news," https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/index.aspx?lang=eng

audience, including to diaspora communities, that RRM announcements are recent phenomenon and quantitatively are few and far between, and that little effort is made to ensure that they have a public impact. Issuing an occasional public statement is simply not enough.

The PIFI final report implicitly recognizes some of the challenges of relying on the small RRM unit at Global Affairs Canada to "detect, deter and counter" foreign digital interference. Its recommendations to create a new open-source intelligence entity in the federal government speaks to the limitations of the RRM, yet fails to do more than suggest that the RRM can provide "expertise" to be shared with the new entity. [82]

As Shelly Ghai Bajaj has noted in a podcast hosted by Marie Lamensch, one interesting finding of her research is that some target diaspora communities are well aware of disinformation circulating in social media spaces they use and have mounted some responses of their own from within their own communities to counter false narratives. [83]

But much more could be done to ensure that diaspora communities are aware of and receptive to RRM Canada announcements and can put them to use in their own community discourses.

INSIGHTS FROM NGO REPORTING

NGOs draw from different sources of information than do government agencies, review bodies and official inquiries. While they don't have access to government holdings of intelligence they do have access to diaspora groups and leaders in ways that can surpass those of government. Given that access, their analysis of Foreign interference and transnational repression is especially valuable.

One example is a study by "Disinfowatch," a NGO dedicated to monitoring disinformation. Its 2024 report on "PRC Foreign Interference and Transnational Repression in Canada" is based on interviews with 25 leaders from communities vulnerable to PRC FI. The report paints a picture of a sophisticated PRC use of "media, community influence and targeted intimidation" to "shape a narrative that marginalizes critics and reinforces control over the Chinese diaspora in Canada."[84] Through its interview program it found that community leaders experienced harassment, intimidation, surveillance and online threats.[85] Its interviewees reported high levels of threats to activists, family members in China, and political pressure, with many reporting offers of financial incentives from PRC proxies. [86]

Disinfowatch found focused targeting directed at the Uyghur, Tibetan Community, Hong Kong and Taiwanese communities, as well as Falun Gong practitioners.

Disinfowatch makes a number of recommendations based on its study, some of which have also been discussed in this paper. They include strengthening engagement with diaspora communities, improving government coordination and transparency, and strengthening community resilience.[87] Their suggestions for dealing with digital TNR involve potential regulation of social media and support for civil society efforts to analyze influence operations. [88]

The NGO "Freedom House," has published a case study of Canada in its series on policy responses to transnational repression. The study notes that mechanisms to report individual threats are "inadequate," and captures the sentiment that "people targeted by transnational repression in Canada

82 PIFI final report, vol. 1, recommendation #11, p. 113

83 https://drive.google.com/drive/folders/1_U0k9YPAkdJnkUd792Zy7J-8Ou5hKDxh

84 Disinfowatch, Marcus Kolga, Sze-Fung Lee and Sarah Teich, "PRC Foreign Interference and Transnational Repression in Canada," Dec. 10, 2024, p.11, https://disinfowatch.org/wp-content/uploads/2024/12/DPS-Disinfowatch-PRC-Foreign-Interference.pdf

85 Ibid., p. 15

86 Ibid, p. 16

87 Ibid., pp. 24-26

88 Ibid

have been disappointed by the lack of response from law enforcement."[89] Like Disinfowatch, the Freedom House report makes some recommendations for improved government capacity, including more training for government officials on TNR issues, and improved outreach activities by the RCMP and CSIS. [90]

Also noteworthy are two independent studies that focus in whole or in part on digital transnational repression. A section of a recent Human Rights Watch report calls particular attention to the use by foreign governments of spyware as a tool of repression. As HRW indicates, "spyware allows access to all of a user's data and essentially turns an infected device, such as a mobile phone, into a portable surveillance tool. "[91] The report also notes that the PRC uses its access to WeChat to pursue surveillance and censorship of its citizens abroad.[92] In addition, HRW details digital TNR practices by Ethiopia, Rwanda and Saudi Arabia. [93]

A more extensive study of digital TNR has been carried out by the Citizen Lab project at the University of Toronto.

Researchers for Citizen Lab identified some key features of digital TNR that make its use attractive for foreign repressive states. They include the seeming low risk attached to such activities, the difficulties of detection of a state guiding hand, both of which perpetrate a lack of accountability; and the widespread chilling effect that can be achieved.[94] Impacts of digital TNR that Citizen Lab uncovered through an interview program include self-censorship, altered behaviours and concerns about threats to the safety of family members in the home country—all examples of the chilling effect.[95]

The Citizen Lab report also identified some of the key methodologies used in digital TNR against Canadian targets. They include "hacking and phishing, account takeovers, troll and bot campaigns on social media, online threats, and disinformation campaigns."[96] These methods are illustrated in anonymized accounts of the experiences of a number of targeted individuals, including those from Saudi Arabia, Hong Kong, Iran, Syria, East Turkestan, Yemen, and the PRC. [97]

The individuals Citizen Lab engaged with also reported significant levels of dissatisfaction with government agency responses to their experiences of digital TNR. Many felt they could not work with law enforcement agencies. [98]

Citizen Lab advances a number of policy recommendations to the government to try to ensure that perpetrators of digital TNR are held to account, including through criminal sanctions. They also propose tougher measures to deal with surveillance technologies, more coordinated government efforts against digital TNR, engagement with social media platforms, and supports for private sector organizations to assist victims of digital TNR. [99]

89 Freedom House, Policy Responses to Transnational Repression, "Case Study Canada," 2022, p. 2, https://freedomhouse.org/report/transnational-repression/canada

90 Ibid., p. 8

91 Human Rights Watch, "We will Find You: A Global Look at How Governments Repress Nationals Abroad," February 22, 2024, p. 30, https://www.hrw.org/report/2024/02/22/we-will-find-you/global-look-how-governments-repress-nationals-abroad

92 Ibid., p. 31

93 Ibid, pp. 32-33.

94 The Citizen Lab, "Psychological and Emotional War: Digital Transnational Repression in Canada," Research Report #151, March 1, 2022, p. 9, https://utoronto.scholaris.ca/server/api/core/bitstreams/84d7937d-3383-48e7-9b0d-51ba9a70b4ef/content

95 Ibid, pp. 10-12

96 Ibid, p. 14

97 Ibid, pp. 14-24

98 Ibid, p. 25

99 Ibid, pp. 28-34

CONCLUSION

NAVIGATING THE WORLD OF FOREIGN INTERFERENCE, TRANSNATIONAL REPRESSION AND DIGITAL DISINFORMATION

If there is one theme that ties together so much of the public reporting on foreign interference, transnational repression and digital influence campaigns it is the importance of greater transparency, public knowledge, and engagement to ensure societal resilience. This was a point emphasized in the PIFI final report. It was blunt in its message that governments needed to be much more transparent with the Canadian public about foreign interference threats. Greater transparency was required to ensure that individuals and communities would be in a position to better understand an evolving threat. There was also the suggestion that better levels of understanding would translate into enhanced societal resilience. But beyond being potential recipients of more Government information, societal resilience was depicted as largely up to individuals and communities to engineer. A better bargain is needed.

What might that better bargain look like?

A SHORT LIST OF WHAT THE GOVERNMENT NEEDS TO DO FOR CANADIANS

A recognition of the importance of transparency regarding foreign interference, disinformation campaigns and transnational repression needs to be delivered through action. More transparency will, however, not be enough on its own. In addition to more transparency, there will be a need for more engagement between the government and affected communities, and more enforcement against foreign interference perpetrators.

There are a host of recommendations that require serious consideration and action, whether from official inquiries, review body reports or expert studies form the NGO community.

I will try to draw out some of the most important here, grouped in three baskets.

1. Transparency deliverables

- *The Canadian public deserves more access to information about FI threats. To remedy current deficiencies the following steps could be taken:*
- *The immediate publication of a foreign interference strategy based on existing work by Public Safety and the RCMP dating back over six years*
- *More, sustained public threat reporting from the national security and intelligence community, The last CSIS report on foreign interference is now over four and a half years old. That is not good enough. There should be an annual threat assessment prepared for Parliament on global threats to national security with dedicated sections on foreign interference, disinformation campaigns, and transnational repression.*
- *There should be a regular series of public reports on transnational repression, including digital TNR, and its impacts in Canada*
- *Public and substantive attribution statements need to be made about known disinformation campaigns*

2. Improved Engagement

- *To create greater trust in government capabilities and foster a stronger belief in the idea that the Canadian government can and will deliver security for all Canadians, the following measures are recommended:*
- *The government needs to strengthen the role of the National Counter Foreign Interference Coordinator and ensure the role has maximum public visibility*
- *The current status of outreach programs by CSIS and the RCMP needs to be assessed, corrective action taken, better coordination ensured, and the intensity, quality and cultural sensitivity of such programs needs to be improved.*
- *As called for in the PIFI final report, an effective, one-stop-shop "hotline" reporting system for FI threats needs to be instigated as a matter of urgency.*
- *An advisory council needs to be established with representatives of leading diaspora groups and NGO advocates to meet with senior government officials on a regular basis to discuss the evolving threat of FI, the government's response, and community resilience needs. The council should be chaired by the NCFIC with a co-chair selected among the civil society members of the council. It should have a regular, quarterly meeting schedule and publish, in a timely fashion, a summary of its discussions*

3. Enforcement

Canadians need not only to have access to more authoritative information about FI, digital disinformation and transnational repression, they need to see that there are real measures in place to deter and counter these threats.

To that end, here are some proposed measures:

- *Improve the capacity of the RCMP as a law enforcement agency to investigate and lay charges*
- *Operationalize the new criminal sanctions against foreign interference and sabotage contained in Bill C-70*
- *Be more proactive in taking measures against officials of foreign states engaged in foreign interference operations, including by declaring them persona non grata and forcing their removal from Canada*
- *Bring the Foreign Influence Transparency Registry (FITR) into operation, as provided for by Bill C-70 while engaging in a strong public communications strategy to explain to Canadian its intent, objectives and enforcement provisions*
- *Require annual review body reporting on the functioning of the FITR*
- *Digital transnational repression: Giving special attention*

If the final report of the Public Inquiry into Foreign Interference is right, that online information manipulation represents future "existential" threat to Canadian democracy, we must turn greater and more focused attention to a key form of its manifestation, which is digital transnational repression. A good starting point has been provided by the Citizen Lab report on digital TNR published in 2022, which offers a series of recommendations to hold perpetrators to account, support victims and engage with private sector companies. [100]

In this playbook, I would suggest three additional measures, one that reaches beyond Canadian borders.

- *Use the creation of an advisory council chaired by the NCFIC as a forum to create a guide for diaspora communities on "Digital transnational repression and you," similar, but with more substance, to the CSIS publication, "Foreign Interference and you." Co-production, with representatives of diaspora groups, of an agreed guide would be very beneficial.*
- *Ensure that the Foreign Influence Transparency Registry provided for in Bill C-70, "An Act Respecting Countering Foreign Interference," can be interpreted through regulation and used as an instrument to deter digital TNR as its applies to political or governmental processes.[101] While this will not capture the broad sweep of digital TNR, it represents a starting point.*
- *Transnational repression is a global phenomenon and there is potentiality in addressing it in a multilateral framework. One such framework could be the G7 group of countries, which decided to tackle disinformation threats on a collective basis in 2018. The G7 could adopt a similar approach to TNR at the summit hosted by Canada in June 2025. This would involve a collective security approach to monitoring of TNR, the sharing of information about perpetration, and the development of mutually agreed policy responses.*

There is no silver bullet to stop or prevent foreign interference, digital disinformation and transnational repression. But there is a requirement to demonstrate serious intent to "detect, deter and counter," in a proportional and democratic manner, the threats involved.

100 Ibid

101 Bill C-70, "An Act respecting countering foreign interference," https://www.parl.ca/DocumentViewer/en/44-1/bill/C-70/royal-assent

APPENDIX

HOTLINES and How to Report Foreign Interference

Canadian Security Intelligence Service, "Reporting national security information." https://www.canada.ca/en/security-intelligence-service/corporate/reporting-national-security-information.html

Public Safety Canada, "How to report foreign interference." https://www.publicsafety.gc.ca/cnt/ntnl-scrt/frgn-ntrfrnc/hr-en.aspx

RCMP, "National Security Information Network," https://rcmp.ca/en/federal-policing/national-security/national-security-information-network

How to Contact your Member of Parliament

https://www.ourcommons.ca/en/contact-us

Public Inquiries and Review Body Reports

Independent Special Rapporteur on Foreign Interference, The Right Honourable David Johnston, First Report, May 23, 2023, https://www.canada.ca/en/democratic-institutions/services/reports/first-report-david-johnston-independent-special-rapporteur-foreign-interference.html

National Security and Intelligence Committee of Parliamentarians, (NSICOP), "Special Report on Foreign Interference in Canada's Democratic Processes and Institutions," June 2024, https://www.nsicop-cpsnr.ca/reports/rp-2024-06-03/special-report-foreign-interference.pdf

Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions (PIFI), website: https://foreigninterferencecommission.ca

Public Inquiry into Foreign Interference, Final Report, January 2025, https://foreigninterferencecommission.ca/reports/final-report

Government of Canada threat assessments

Canadian Security Intelligence Service Annual Public Report, 2023, published May 2024, https://www.canada.ca/content/dam/csis-scrs/documents/publications/Public_Report_2023-eng-DIGITAL.pdf

Canadian Security Intelligence Service, "Foreign Threats to Canada's Democratic Processes," July 2021, https://www.canada.ca/content/dam/csis-scrs/documents/publications/2021/foreign-interference-threats-to-canada%27s-democratic-process.pdf

CSE, "Cyber Threats to Canada's Democratic Processes, 2025 Update," https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-2025-update

CSE, "Cyber Threats to Canada's Democratic Processes, 2023 Update," https://www.cyber.gc.ca/sites/default/files/cyber-threats-canada-democratic-process-2023-update-v1-e.pdf

CSE/Canadian Centre for Cyber Security, "National Cyber Security Threat Assessment 2024-2025", https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf

Government of Canada guidance

Canadian Centre for Cyber Security (CCCS), "How to Identify misinformation, disinformation and malinformation," https://www.cyber.gc.ca/sites/default/files/misinformation-mesinformation-itsap.00.300-en.pdf

Canadian Centre for Cyber Security (CCCS), https://www.cyber.gc.ca/en

CCCS, "Get Cyber Safe," https://www.getcybersafe.gc.ca/en

CSIS, "Foreign Interference and You," https://www.canada.ca/en/security-intelligence-service/corporate/publications/foreign-interference-and-you/foreign-interference-and-you.html

Global Affairs Canada, "Rapid Response Mechanism," https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/index.aspx?lang=eng

Government of Canada, "Countering an Evolving Threat: Update on recommendations to counter foreign interference in Canada's democratic institutions," March 2023, https://www.canada.ca/en/democratic-institutions/services/reports/countering-evolving-threat.html

Government of Canada, "Combatting Foreign Disinformation and information manipulation," https://www.canada.ca/en/democratic-institutions/services/reports/countering-evolving-threat.html

Privy Council Office, "Canada's Intelligence Priorities," September 2024, https://www.canada.ca/en/privy-council/services/publications/canada-intelligence-priorities.html

Public Safety, "Foreign Interference and Canada," https://www.canada.ca/en/public-safety-canada/news/2024/05/foreign-interference-and-canada.html

RCMP, "Foreign Actor Interference," https://rcmp.ca/en/federal-policing/national-security/foreign-actor-interference

Institutional Reports

CSIS Institutional Report, PIFI database, CAN.DOC.000044, https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Exhibits_and_Presentations/Exhibits/CAN.DOC.000044.pdf

RCMP Stage 2 Institutional Report, CAN.DOC.000042, https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Exhibits_and_Presentations/Overview_Institutional_Reports/CAN.DOC.000042.pdf

Disinformation

Carnegie Endowment for International Peace, "Countering Disinformation Effectively: An Evidence-Based Policy Guide," January 31, 2024, https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide?lang=en

Government of Canada, "Learn about online disinformation", https://www.canada.ca/en/campaign/online-disinformation/learn-about-it.html

OECD (Organisation for Economic Cooperation and Development), "Mis-and Disinformation," https://www.oecd.org/en/topics/sub-issues/disinformation-and-misinformation.html

RAND Insight report, "The Russian 'Firehose of Falsehood' Propaganda Model,' July 11, 2016, https://www.rand.org/pubs/perspectives/PE198.html

Independent Sources on foreign interference, disinformation and transnational repression

Amnesty International, "Students at Canadian Universities face surveillance, harassment by Chinese state authorities," May, 2024, https://amnesty.ca/human-rights-news/students-canadian-universities-surveillance-harassment-chinese-state-authorities/

Centre for International Governance Innovation, Submission to the Public Inquiry, https://www.cigionline.org/publications/final-submission-to-the-public-inquiry-into-foreign-interference-in-federal-electoral-processes-and-democratic-institutions-in-canada/

The Citizen Lab, "Psychological and Emotional War: Digital Transnational Repression in Canada," Research Report #151, March 1, 2022, p. 9, https://utoronto.scholaris.ca/server/api/core/bitstreams/84d7937d-3383-48e7-9b0d-51ba9a70b4ef/content

Digital Public Square, "Public Opinion Survey of Foreign interference in Canada," November 14, 2024, https://www.digitalpublicsquare.org/insights/survey-from-the-foreign-interference-resilience-education-project?fbclid=PAZXh0bgNhZW0CMTEAAaYMrcpF_9ZWpT1L5OlzRLAWyOZSwT96Lhawe2zyAvvSjmReqE2nIYjf7DU_aem_YTeUrHgs6Pey0wW_SZH4Dw

Disinfowatch, Marcus Kolga, Sze-Fung Lee and Sarah Teich, "PRC Foreign Interference and Transnational Repression in Canada," Dec. 10, 2024, p.11, https://disinfowatch.org/wp-content/uploads/2024/12/DPS-Disinfowatch-PRC-Foreign-Interference.pdf

Freedom House, "Transnational Repression," https://freedomhouse.org/report/transnational-repression

Freedom House, Policy Responses to Transnational Repression, "Case Study Canada," 2022, p. 2, https://freedomhouse.org/report/transnational-repression/canada

Human Rights Watch, "We will Find You: A Global Look at How Governments Repress Nationals Abroad," February 22, 2024, p. 30, https://www.hrw.org/report/2024/02/22/we-will-find-you/global-look-how-governments-repress-nationals-abroad

Legislation

Bill C-70, An Act Respecting Countering Foreign Interference, June 2024, https://www.parl.ca/DocumentViewer/en/44-1/bill/C-70/royal-assent

Canadian Security Intelligence Service Act, https://laws-lois.justice.gc.ca/pdf/c-23.pdf

Montreal Institute for Global Security, podcast series

As part of the Canadian Digital Defenders Collective, MIGS conducted seven interviews with Canadian and international experts. The interviews aim to equip the audience with a critical knowledge of mis- and disinformation, online harms and other foreign interference and transnational repression through information and conversations, particularly in a Canadian context. The interviewees bring examples of Canadian instances of online harms and foreign influence to raise awareness about the fact that these harms exist in Canada and can be mitigated. All episodes of "Human Rights Talks" are available on iTunes, Spotify and Podbean.

"Hong Kong: Escalation of Transnational Repression against Hong Kongers in Canada" - Interview with Katherine Leung, Policy Advisor at Hong Kong Watch. Interview dated March 2, 2025.

"Influence étrangère au Québec et au Canada : YouTube, Tik Tok, WeChat et ces applications qui passent sous le radar" – Interview with Nicholas de Rosa, journalist at Radio Canada. Interview dated February 29, 2025

"The Real-Life Impact of Transnational Repression: Iranian activist Maryam Shafipour Speak out" – interview with Maryam Shafipour, Iranian human rights activist. Interview dated February 6, 2025.

"Messaging Apps and the Spread of Disinformation" – Interview with Samuel Wooley, Dietrich Endowed Chair in Disinformation Studies at the University of Pittsburg. Interview dated February 4, 2025.

"Digital Transnational Repression in Canada: When the Chinese Government Targets the Diaspora" – interview with Sam Cooper, award-winning investigative journalist and best-selling author. Interview dated January 27, 2025.

"Digital Diasporas, Messaging Apps and the Transnational Disinformation Threats" – interview with Shelly Ghai Bajaj, Postdoctoral Fellow at the University of Waterloo. Interview dated January 20, 2025.

"Répression transnationale et influence étrangère au Canada" - interview (in French) with Fanny Tan, tech journalist and researcher at the l'Observatoire des conflits multidimensionnels at the Chaire Raoul Dandurand at UQAM. Interview dated January 17, 2025.

Links to diaspora community advocacy groups

Canadian Council for Refugees, "CCR Member Organizations," https://ccrweb.ca/en/members

List of Ethnic Interest Groups in Canada, https://en.wikipedia.org/wiki/List_of_ethnic_interest_groups_in_Canada

Panel Physician, "A Guide to Finding Immigrant Organizations in Canada," https://www.panelphysician.ca/blog/finding-immigrant-organizations-in-canada

ABOUT THE AUTHOR

Wesley Wark is a senior Fellow at the Centre for International Governance Innovation, in Waterloo, Canada, where he co-directed a major project on Canadian National Security Strategy. He is co-author of the CIGI special report published in 2021, "Reimagining a Canadian National Security Strategy."

Professor Wark served as a member of the Prime Minister's Advisory Council on National Security for two terms (2005-2009) and on the President of the Canada Border Services Agency's Advisory Committee (2006-2010). He was an advisor to the Minister of Public Safety on national security policy and legislation between 2015 and 2019. He is the co-lead for the submissions provided by the Centre for International Governance Innovation to the current Public Inquiry on Foreign Interference, and wrote an expert report for the Public Order Emergency Commission.

He spent most of his academic career at the University of Toronto, where he taught from 1988 to 2013. Prior to joining the University of Toronto, he taught at the London School of Economics, McGill University and the University of Calgary. He holds a Ph.D. from the London School of Economics and an M.A. from Cambridge University. He currently teaches professional courses on intelligence and security and on national security and intelligence review offered through the Balsillie Executive Institute. He is a fellow at the Balsillie School of International Affairs

He is a frequent contributor to the Canadian media on national security issues and is often invited to appear before Parliamentary committees to give testimony. He has published widely in the field of intelligence and national security studies. He writes a newsletter on national security and intelligence issues, available at: wesleywark.substack.com

ABOUT THE MONTREAL INSTITUTE FOR GLOBAL SECURITY

The Montreal Institute for Global Security is a non-partisan think tank and Canada's leading source of actionable research and analysis on global conflicts, emerging technologies, and human rights. Led by experts in security, geopolitics, human rights and digital threats, the Institute supports policymakers, businesses, and civil society in navigating today's complex and evolving security landscape marked by an alignment of authoritarian actors. Our work spans countering transnational repression, safeguarding democracy from authoritarian influence, addressing challenges in cyberspace and ensuring AI and emerging technologies are used in a responsible manner. By integrating cutting-edge research with real-world impact, we provide high-precision intelligence to help organizations and governments respond effectively to evolving global threats, available at: migsinstitute.org

This report is made possible by the generous support
of the Department of Canadian Heritage.

MIGS Montreal Institute for Global Security

Canadian Heritage Patrimoine canadien