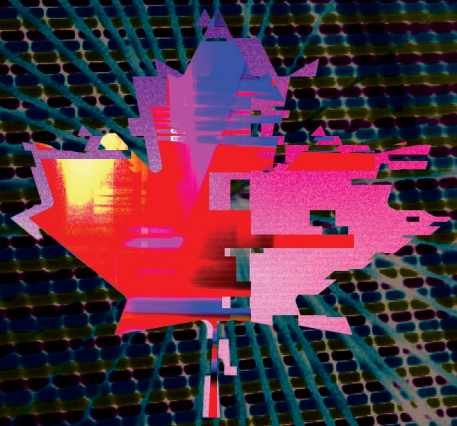
Centre for International
Governance Innovation

Final Submission to the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions in Canada



Wesley Wark and Aaron Shull

Centre for International
Governance Innovation

Final Submission to the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions in Canada

Wesley Wark and Aaron Shull

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director and General Counsel Aaron Shull
Director, Program Management Dianna English
Program Manager and Research Associate Kailee Hilt
Publications Editor Susan Bubak
Senior Publications Editor Jennifer Goyder
Graphic Designer Sami Chouhdary

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Authors

Wesley Wark is a senior fellow at CIGI and a fellow with the Balsillie School of International Affairs. His academic career included teaching at McGill University, the University of Calgary and the University of Toronto. He served two terms on the prime minister of Canada's Advisory Council on National Security (2005–2009) and on the Advisory Committee to the President of the Canada Border Services Agency (2006–2010). More recently, he provided advice to the minister of public safety on national security legislation and policy. He has appeared on numerous occasions before parliamentary committees and comments regularly for the media on national security issues.

He is the co-editor (with Christopher Andrew and Richard J. Aldrich) of *Secret Intelligence: A Reader*, second edition (Routledge, 2019). He co-led the major CIGI project on Reimagining a Canadian National Security Strategy and wrote, with Aaron Shull, its capstone report. He was the series editor, with Aaron Shull, of the CIGI digital essay series Security, Intelligence and the Global Health Crisis. He is a former editor of the journal *Intelligence and National Security* and now serves on the journal's advisory board.

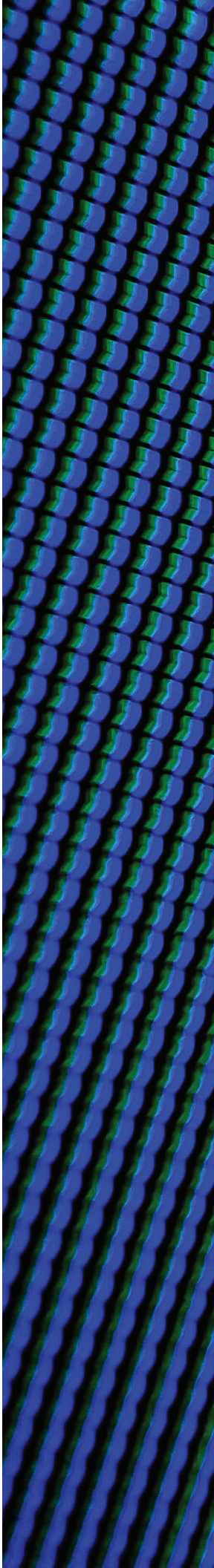
Aaron Shull is the managing director and general counsel at CIGI. He is a senior legal executive and is recognized as a leading expert on complex issues at the intersection of public policy, emerging technology, cybersecurity, privacy and data protection.

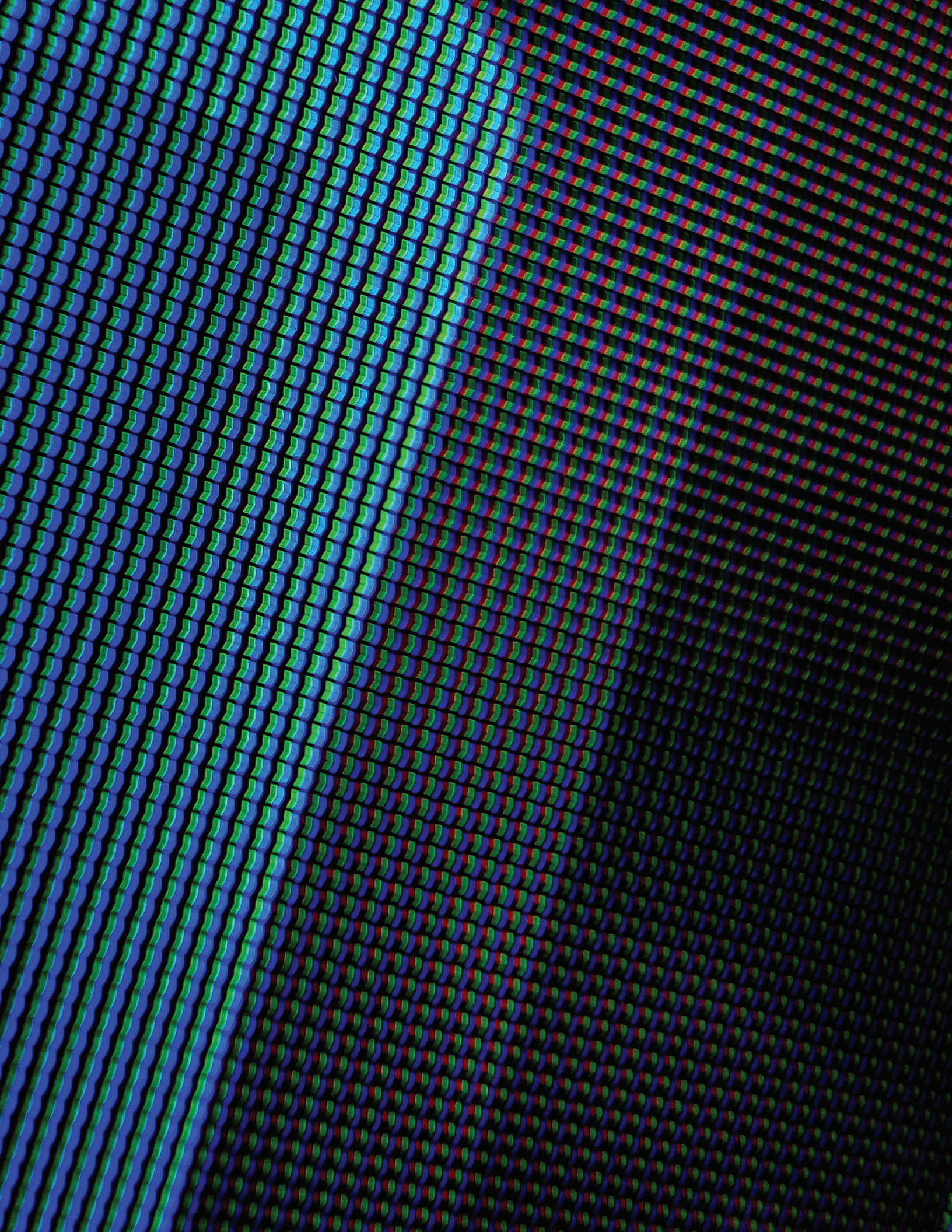
Aaron has extensive experience building global networks of experts to enhance engagement with researchers and practitioners drawn from government, academia, industry and civil society. He recently concluded the project Reimagining a Canadian National Security Strategy, which was unprecedented in scale and scope in Canada. It engaged a multidisciplinary network of more than 250 experts to inspire updated and innovative national security and intelligence practices and offered a series of key policy recommendations to assist the Government of Canada in addressing the challenges of a new security environment.

This work was well received by senior officials in government and inspired public conversations with Canada's minister of public safety; the national security and intelligence advisor to the prime minister of Canada; the director of the Canadian Security Intelligence Service; the chief of the Communications Security Establishment; and the privacy commissioner of Canada.

Acronyms and Abbreviations

ADM	assistant deputy minister
CIGI	Centre for International Governance Innovation
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
G7	Group of Seven
GAC	Global Affairs Canada
IAS	Intelligence Assessment Secretariat
MPs	members of Parliament
NCFIC	national counter foreign interference coordinator
NIC	National Intelligence Community
NSI	national security and intelligence
NSIA	national security and intelligence adviser
NSICOP	National Security and Intelligence Committee of Parliamentarians
NSIRA	National Security and Intelligence Review Agency
NSS	National Security Strategy
NSTC	National Security Transparency Commitment
OSINT	open-source intelligence
PCO	Privy Council Office
PIFI	Public Inquiry into Foreign Interference
PROC	Standing Committee on Procedure and House Affairs
RCMP	Royal Canadian Mounted Police
RRM Canada	Rapid Response Mechanism Canada
SECU	Standing Committee on Public Safety and National Security
SITE	Security and Intelligence Threats to Elections Task Force
TS	top secret





Consolidated List of Recommendations

The Public Inquiry into Foreign Interference (PIFI) is a critical initiative aimed at addressing foreign interference and strengthening national security in Canada. PIFI's mandate includes evaluating current policies, practices and systems that address foreign interference; enhancing transparency; and recommending improvements for more effective governance.

Our recommendations reflect a need to achieve higher levels of **strategic transparency** concerning foreign interference threats, the value of a further **systematic review** of the Canadian national security and intelligence (NSI) system, **targeted improvements** to the capacity of the NSI community, and measures to achieve greater **political actor literacy** on foreign interference threats.

The following recommendations provide a framework for advancing these objectives.

Recommendation 1: The PIFI final report should recommend that the government publicly restate a commitment to the National Security Transparency Commitment (NSTC), re-energize its work and promote it across government, including in ministerial mandate letters for all NSI-relevant departments. Delivery of its goals needs to be accounted for on an annual basis, thus allowing for greater public accountability about progress on national security accountability. This accountability could include existing governance mechanisms, such as annual plans and priorities reports.

Recommendation 2: The government should produce an updated public foreign interference strategy, drawing on previous work done by Public Safety Canada, and on the work of PIFI, and accompany it with a strong strategic communications policy to ensure that it is available to communities targeted by foreign interference in Canada as well as the general public. Indeed, one of the purposes of the public strategy should be to draw general attention to the ways in which foreign interference affects targeted individuals and communities.

Recommendation 3: The Inquiry should reference the importance of producing the promised National Security Strategy (NSS) in as short a time frame as possible and that it be accompanied by a robust strategic communications plan, so that the strategy may properly enter the public discourse. We also suggest a number of elements that should accompany the production of an NSS, namely, that:

- PIFI should recommend that production of an NSS be part of a mandate letter for the appropriate minister;
- the NSS be understood as being a responsibility of the NSI adviser (NSIA) to the prime minister;
- the public release of the NSS include a cover letter from the prime minister spelling out their view of its importance to Canadians; and
- future governments commit to a plan to produce an NSS on a four-year cycle.

Recommendation 4: PIFI should recommend to the government that it publishes a redacted version of the Intelligence Assessment Secretariat's (IAS's) *National Security Outlook* report on an annual basis, under the auspices of the NSIA.

Recommendation 5: PIFI should recommend to the government that it generate a governance plan for the declassification and release, in the public interest, of important records related to national security. The PIFI further recommends that the government create an advisory body of outside experts to assist in strategic determinations about records declassification and release.

Recommendation 6: PIFI should recommend to the government the need for an independent expert review of the Canadian NSI system as a whole. The Australian model can provide guidance for its conduct.

Recommendation 7: PIFI should recommend the construction, strengthening and ongoing maintenance of an integrated intelligence fusion centre at the Privy Council Office (PCO), built on the expansion of the IAS, and capable of the regular production of reports that integrate domestic and international security issues. The intelligence fusion centre will serve, under the direction of the NSIA, as a major resource for the National Security Council of Cabinet.

Recommendation 8: PIFI should recommend to the government the creation of an open-source intelligence (OSINT) centre of expertise with appropriate mandate and authorities.

Recommendation 9: PIFI should support the relocation of the foreign disinformation tracking unit (Rapid Response Mechanism Canada [RRM Canada]) from Global Affairs Canada (GAC) to Public Safety or the PCO. RRM Canada needs a clear mandate, including for public attribution of foreign state information operations, and much greater resources.

Recommendation 10: PIFI should recommend that the new office of the national counter foreign interference coordinator (NCFIC) be strengthened, provided with additional resources, be fully connected to intelligence reporting, and develop a coherent strategic plan for public outreach, education and parliamentary engagement.

Recommendation 11: PIFI should emphasize the importance of the role of the NSIA and recommend strengthening the function with several measures, including creating a profile for the office holder and having the prime minister provide the NSIA with a mandate letter. A stronger secretariat capacity is required for the NSIA to perform a coordination role for the NSIA community, be a key disseminator of intelligence to the prime minister and Cabinet, and function as the top representative of the Canadian NSI community with Five Eyes partners (Australia, Canada, New Zealand, the United Kingdom and the United States) and others.

Recommendation 12: PIFI should recommend that the minister of public safety develop and publish a strategic plan for reform of Royal Canadian Mounted Police (RCMP) federal policing to ensure that it can be effective in dealing with foreign interference threats in the future.

Recommendation 13: The Centre for International Governance Innovation (CIGI) commends the Inquiry for undertaking an independent examination of the National Security and Intelligence Committee of Parliamentarians (NSICOP) report on foreign interference and for standing on appropriate principles to refuse to "name names." CIGI recommends that PIFI include a substantive, compelling analysis, using a "write to release" approach, of the allegations contained in the NSICOP report and that its analysis be referred to relevant standing committees in the House (the Standing Committee on Public Safety and National Security [SECU] and the Standing Committee on Procedure and House Affairs [PROC]) and Senate (the Committee on National Security and Defence) as well as to NSICOP, for further study.

Recommendation 14: CIGI suggests that PIFI recommend in its final report a series of steps to improve Parliament's ability to understand foreign interference and other national security steps. In particular, we recommend that the Security and Intelligence Threats to Elections (SITE) Task Force establish an enhanced ability to share meaningful classified intelligence with security-cleared members of the parties during the writ period and that the SITE Task Force after-action report following a general election be declassified and published. We recommend that the commissioner include a strong recommendation in her final report urging Parliament to proceed, as a matter of urgency, to accomplish the delayed statutory reviews of the legislation that governs the activities of the key independent review bodies, NSICOP and the National Security and Intelligence Review Agency (NSIRA). Finally, the commissioner should recommend that a budget be allocated by Parliament to all recognized political parties in the House and groups in the Senate to allow them to hire and maintain a dedicated security-cleared officer to act as an internal party expert resource on foreign interference and, more broadly, national security threats.

CIGI's Full Written Submission

CIGI applied for and was granted standing in the policy phase of PIFI (2024a, 184). In the decision to grant standing, Commissioner Marie-Josée Hogue noted that "its participation would provide a unique, interdisciplinary perspective on a range of issues within the Commission's mandate. Given CIGI's extensive background and expertise in matters such as national security, cybersecurity and democratic institution resilience, I am satisfied that it has a sufficiently substantial connection and could make a necessary contribution to the Commission's policy work" (PIFI 2024b, 63).

This special report represents CIGI's final written submission to the Inquiry. It was preceeded by earlier written submissions in response to requests from the PIFI Research Council and by a brief oral closing submission presented to the commissioner on October 24, 2024. In preparing this written submission, CIGI benefited from a close study of the report of the independent special rapporteur, the PIFI interim report and the Commission's public hearings, the redacted versions of the special reports on foreign interference published by NSIRA and NSICOP, and the voluminous declassified records made available through the Commission process.

CIGI convened two independent, invitation-only round tables to gather insights on foreign interference: one comprising former officials and the other consisting of current members of the NSI community. We are grateful for their valuable contributions and perspectives. However, it is important to emphasize that this written submission represents CIGI's views alone. Our goal throughout has been to cultivate an objective understanding of these issues and to present a balanced, non-partisan perspective.

This submission responds to clause E of the Commission's terms of reference to recommend "any means for better protecting federal democratic processes from foreign interference."[1] It will be organized into six parts:

- the need for greater federal government strategic transparency and public education efforts regarding foreign interference and wider national security threats;
- the need for enhancements to the federal government's capacity to detect, deter and counter foreign interference threats, including disinformation;
- intelligence dissemination challenges and reforms;
- the role of the RCMP as a key actor in national security and countering foreign interference;
- the need for an analysis of the significance of the NSICOP special report on foreign interference's findings regarding the alleged complicity of parliamentarians in foreign interference schemes; and
- the importance of enhanced political actor literacy about foreign interference threats, and national security more broadly.

To provide context for this submission, we begin with observations on the NSI community, recognizing the professionalism, dedication and integrity of the public servants who work tirelessly each day to make Canada safer for all.

The NSI community is a bureaucracy, as former NSIA Richard Fadden reminded the Commission (PIFI 2024c). Yes, of course. Bureaucracies have been the subject of study since the pioneering work of German sociologist Max Weber a century ago. What is of interest are the special characteristics of the NSI as a bureaucracy. We note that the community is historically siloed and decentralized. Coordination of the community has been a challenge since its initial elements were created after the Second World War. A second feature is that change to the practices of the NSI community tends to be orchestrated in an incremental fashion and often based on a study of best practices on the part of our Five Eyes partners. This habit can produce solid proposals for reform; it can also make the NSI community less nimble than it needs to be, especially in the face of a rapidly evolving and deepening security threat environment. A third characteristic is that the NSI community is inevitably wedded to the protection of secrets and may struggle to fully appreciate the value of transparency, review and declassification protocols.

While significant progress has been made to change a culture of secrecy, more work needs to be done. A final factor, not unique to the Canadian community, but still posing a significant problem, concerns the friction involved in what is often called the intelligence "producer-consumer" relationship. What this references, and it is much studied in the literature on intelligence, is the need for a well-honed process, and associated culture, to ensure that relevant intelligence reports and briefings are circulated in a timely manner to decision makers at both the official and political levels. Such reporting depends not just on dissemination practices for its success but also on the understanding by "consumers" of the nature and significance of intelligence products and a willingness to devote serious attention to it. In making recommendations to the Inquiry, these characteristics of the NSI system will be kept in mind.

1 See www.canada.ca/en/democratic-institutions/general/terms-reference.html.

Achieving Greater Strategic Transparency

One of the key challenges facing the Inquiry in its fact-finding role is to provide the public with an evidence-based and clear-eyed assessment of the impacts of foreign interference on Canada's general elections and democratic processes over the past six years. This task has fallen to PIFI following a course of events, beginning with unauthorized leaks of classified intelligence to the media starting in the fall of 2022, and culminating with the release of the NSICOP special report in June 2024, which has created a state of understandable public confusion and, in some quarters, loss of trust in the integrity of Canada's elections and its Parliament.

The current state of confusion in the public sphere has not arisen from a lack of government efforts to inform the public about the national security threats posed by foreign interference — quite the opposite. Yet these efforts have not been sufficient to counter a growing confusion about the impacts of foreign interference. This situation necessitates a reassessment of how the government conceptualizes and communicates NSI issues to the public.

It is our view that sustained efforts must be made by the federal government to achieve what we will call **strategic transparency**. Strategic transparency is not an end in itself but a vital means to an end. Strategic transparency involves the systematic publication of core overall strategies and policies on national security issues — these are the means. The objective is to be able to give Canadians a holistic picture of national security threats, government policy and responses, and illustrate how these operate to defend Canadian democracy and protect Canada's national interests. Strategic transparency is a vital tool for building public awareness and allowing for the exercise of accountability. It is also a way to bring coherence to what might otherwise be a very disparate and, for Canadians, very confusing picture. These are the ends to be pursued through strategic transparency.

The importance of improved strategic transparency is not lost on the federal government. It is, in fact, a familiar concern and was at the heart of the first-ever NSTC, issued in 2017, alongside the introduction of major legislation on national security (Bill C-59).[2]

The NSTC advanced six principles, grouped under three themes: information transparency; executive transparency; and policy transparency. The policy transparency theme, and its incorporated principle 5, speaks directly to the need for strategic transparency. Principle 5 states: "The Government will inform Canadians of the strategic issues impacting national security and its current efforts and future plans for addressing those issues."[3]

Why put a focus on this? The NSTC suggests knowledge of strategic issues will put other transparency initiatives "into context."

In our view, that is too modest an expression of purpose. What "knowledge of strategic issues" means for Canadians is essentially the opportunity to grasp the big picture of national security.

There are ongoing efforts to deliver on the promise laid out in the NSTC and its various principles. On September 19, 2024, the Government of Canada published, for the first

2 See www.canada.ca/en/services/defence/nationalsecurity/national-security-transparency-commitment.html.

3 See www.canada.ca/en/services/defence/nationalsecurity/national-security-transparency-commitment/policytransparency.html.

time, its intelligence priorities. The public document explicitly referred to the NSTC as a guiding rationale for the publication and embedded the list of intelligence priorities in a larger context of explaining the fundamentals of intelligence, providing an overview of the role of intelligence and a description of the key departments and agencies involved.

Among the 14 intelligence priorities approved by Cabinet, the first listed was "foreign interference and malign influence." A sidebar text included a quote from then Canadian Security Intelligence Service (CSIS) Director David Vigneault, stating, in a speech hosted by CIGI on February 9, 2021, that "the greatest strategic threat to Canada's national security comes from hostile activities by foreign states" (Government of Canada 2024, 19).

The intelligence priorities report concludes with a promise that "the Government is committed to continue working closely with Canadians, as well as review and oversight bodies, to increase public knowledge, awareness, and understanding [of] the activities of the national security and intelligence community" (ibid., 23).

Given this context, recommendations for enhancing strategic transparency in national security may seem redundant; however, we believe further action is essential. Greater efforts are needed to fully embed the NSTC into government practices and to ensure consistent public reporting that keeps Canadians informed about the strategic threat landscape and policy responses.

Recommendation 1: The PIFI final report should recommend that the government publicly restate its commitment to the NSTC, re-energize its work and promote it across government, including in ministerial mandate letters for all NSI-relevant departments. Delivery of its goals needs to be accounted for on an annual basis, thus allowing for greater public accountability about progress on national security accountability. This accountability could use existing governance mechanisms, such as annual plans and priorities reports.

Being able to create performance metrics for the NSTC would also facilitate more comprehensive reviews that might be conducted in future by NSICOP and/or the National Security Transparency Advisory Group.

Despite the commendable public reporting in recent years by core NSI agencies such as CSIS and the Communications Security Establishment (CSE), exemplified in the annual *CSIS Public Report*, in the CSIS report from July 2021 on *Foreign Interference Threats to Canada's Democratic Process*, and in the series of CSE/Canadian Centre for Cyber Security national cyberthreat assessments, we believe that there is a missing strategic piece to serve as a chapeau for these agency-specific products.

One of the most serious gaps in national security transparency has been the failure of the Public Safety department over a six-year period to publish a foreign interference strategy. A similar fate befell the publication of a related RCMP strategy. Minister of Public Safety Dominic LeBlanc's suggestion to the Inquiry that the government might revisit publishing the foreign interference strategy, based on the Commission's report, should be seized on and made a recommendation.

Recommendation 2: The government should produce an updated public foreign interference strategy, drawing on previous work done by the Public Safety department, and on the work of PIFI, and accompany it with a strong strategic communications policy to ensure that it is available to communities targeted by foreign interference in Canada as well as the general public. Indeed, one of the purposes of the public strategy should be to draw general attention to the ways in which foreign interference affects targeted individuals and communities.

We advance this recommendation because we feel that the draft foreign interference strategy of September 2, 2020, released to the Inquiry, was a strong product that successfully conveyed the breadth of the foreign interference threat and the particular vectors of Canadian society and governance that it targeted, including interference against election and democratic processes, but covering, in addition, four other areas: economic prosperity; international affairs and defence; social cohesion; and critical infrastructure. The draft strategy also named some of the key foreign interference actors, including Russia, China and India. The purpose of the public version of the strategy was to foster enhanced understanding and societal resilience across all levels of governments, stakeholders and the general public (PIFI 2020).

As important as published strategies to deal with specific threats are, there is an equal or greater need to publish an integrated NSS that would cover the waterfront of national security threats and responses. The first — and only — national security policy, *Securing an Open Society*, was published 20 years ago in the aftermath of the September 11 attacks. It is out of date and has been shelved (literally, at Library and Archives Canada).

The government's recent defence policy update, *Our North, Strong and Free*, issued on April 8, 2024, another example of a sectoral strategy document, includes a promise to produce an overarching NSS every four years (Department of National Defence 2024). This work is currently being undertaken by the PCO, led by the assistant secretary to the Cabinet, Security and Intelligence.

We commend the government for this commitment but also would encourage PIFI to underscore its importance and the need for timeliness in a recommendation. Discussion of foreign interference threats and responses will be a core element of the strategy.

Recommendation 3: The Inquiry should reference the importance of producing the promised NSS in as short a time frame as possible and stress that it be accompanied by a robust strategic communications plan, so that the strategy may properly enter the public discourse. We also suggest a number of elements that should accompany the production of an NSS, namely, that:

- PIFI should recommend that production of an NSS be part of a mandate letter for the appropriate minister;
- the NSS be understood as being a responsibility of the NSIA to the prime minister;
- the public release of the NSS include a cover letter from the prime minister spelling out their view of its importance to Canadians; and
- future governments commit to a plan to produce an NSS on a four-year cycle.

In addition, we want to call PIFI's attention to the testimony of Martin Green, former assistant secretary to the Cabinet, Intelligence Assessment. Green discussed a particular IAS reporting product called the *National Security Outlook*, an annual report typically issued in January. It is the continuation of a long tradition, dating back to the late 1990s, of producing what used to be called the "year ahead" intelligence summary by IAS. Green remarked that he thought it would be valuable to produce a public version of this document to inform Canadians about the nature of global security threats, in line with the practice of many of our Five Eyes partners (PIFI 2024d, 19).

We believe that an unclassified version of the *National Security Outlook* report should be prepared and published under the auspices of the NSIA. While it might not rival in scope the annual worldwide threat assessment published by the Office of the Director of National Intelligence (2024) in the United States, as mandated by Congress, it would

fulfill the same function of educating the Canadian public, providing a Canadian outlook on global threats to allies and their publics, and sending a message to adversaries about attention to hostile state and non-state activities (New Zealand Security Intelligence Service 2024).

Recommendation 4: The government should publish a redacted version of the IAS *National Security Outlook* report on an annual basis, under the auspices of the NSIA.

The practicality and value of being able to discuss national security issues in a public setting have been demonstrated in PIFI's work to a remarkable degree. The commissioner's insistence on maximum permissible transparency has allowed for the declassification of sensitive intelligence records, for the release of some cabinet confidences, for the production of records of in camera examinations and the creation of intelligence summaries based on the holdings of the NSI community. These achievements must not be lost.

We believe the PIFI final report should include a recommendation for the creation of a first-ever systematic regime for the declassification and release, in the public interest, of important records related to national security. Such a process would allow for better-informed scholarship, enhanced understanding by thought leaders, improved media attention and reporting, and, ultimately, greater public knowledge. It would also position the federal government to utilize declassified intelligence to better promote and protect Canadian interests internationally. Its value was shown in efforts by key allies, the United States and the United Kingdom in particular, to disseminate intelligence proactively about Russian plans to invade Ukraine.

Recommendation 5: The government should generate a governance plan for the declassification and release, in the public interest, of important records related to national security. To facilitate this, the government should create an advisory body of outside experts to assist in strategic determinations about records declassification and release.

We recognize that the production of strategic public reports on national security issues is resource-intensive and can be challenging. It is important that they be seen not as political products, but as the work of the NSI community itself. We believe they are an important mechanism for enhancing public understanding of national security threats but also have complementary uses to serve:

- as a road map for government activity;
- as an accountability mechanism, including for Parliament;
- as a foundational resource for the independent review bodies;
- as a way to publicly signal Canada's outlook to allies; and
- as a way to warn adversaries.

Public trust in NSI agencies remains fragile in some segments of the population and may even have been undermined by controversies swirling around the government's response to foreign interference. Trust in government has layers. One involves trust in the government of the day; separately, there is the question of trust in the professional institutions of government and its officials. But distrust of one layer can easily bleed into distrust of another. Canada must never come to a point where conspiracy thinking about a "deep state" takes hold, as it has to a degree in the United States. Moving to a regularized process of publishing strategic reports on national security issues may help build, or rebuild, missing public trust in the professional NSI community.

The multiple uses of national security strategic publications are well understood, especially by our Five Eyes partners. The United States engages in a robust production of them. The United Kingdom has produced an integrated review of security, defence, development and foreign policy priorities and updated it over the past few years. Canada has been, to date, a laggard by comparison. That must change.

National security strategic transparency is an important input to public discourse and an integral building block for societal resilience. Finding ways to better communicate such reports to Canadians — to get the message out, beyond sticking them on a website in the two official languages, with drops often timed outside the news cycle — will be vital. The aim should be to establish them as a framework and reference point for public understanding.

Enhancements to the Ability of the NSI System to Detect, Deter and Counter Foreign Interference

The commissioner faces the daunting challenge of making actionable recommendations to improve the performance of the NSI system. This goes to the heart of clause E of the Inquiry's terms of reference. Making such recommendations could have an important impact on public trust in the security institutions of the federal government.

We believe it would be appropriate for the commissioner to call for a further expert systematic review of the NSI system as a whole. The review process should be supported by the PCO and reported to the NSIA in both a classified and redacted version, the latter for public release.

Recommendation 6: The government should undertake an independent expert review of the Canadian NSI system as a whole. The Australian model can provide guidance to its conduct.

No such review has ever been conducted in the modern history of Canadian intelligence, dating back to the end of the Second World War. We believe it should be modelled on the practice in Australia, which has now been tested on several occasions, and could serve as an important complement to the selected framework and activity reviews conducted by NSICOP.

CIGI first advocated for an independent review as part of its major project, Reimagining Canadian National Security. The expert group on intelligence reform, led by Greg Fyffe, a former assistant deputy minister (ADM) who led the PCO IAS between 2000 and 2009, produced a report in November 2021 titled *Prepared: Canadian Intelligence for the Dangerous Decades*, which laid out the reasons for a systemic review.[4]

The Australian government is currently completing an independent review that was commissioned in 2023, following a previous review published in 2017. This independent review initiative was a product of recommendations made on the performance of the

4 See Fyffe (2021).

Australian intelligence system in the aftermath of the 2003 Iraq war. No similar lessons-learned exercise was conducted for the Canadian NSI community.

The terms of reference of the current Australian review offer an excellent model. They include "how effectively the NIC [Australia's National Intelligence Community] serves, and is positioned to serve, national interests and the needs of Government."[5]

As well, the independent review will study issues concerning the outcomes of major investments in Australian intelligence since 2017; make an evaluation of intelligence community workforce needs; interrogate NIC "preparedness in the event of regional crisis and conflict;" look at the effectiveness of classification systems; and examine current oversight and evaluation mechanisms to gauge their effectiveness and consistency across the NIC.[6]

Every one of those lines of study are pertinent, in our view, to the needs of a Canadian independent review.

CIGI also suggests a range of targeted recommendations, which could be advanced independently, as well as being folded into the terms of reference of the larger systematic review.

Creation of an Intelligence Assessment Capacity at PCO Capable of the Systematic Fusion of Domestic and International Threat Reporting

The need for such a capacity was demonstrated during the response to the events of the Freedom Convoy protests. Efforts were made at the time to have PCO IAS function in that role given the absence of such a fusion capacity in the NSI system (Wark 2022). The need for such a capability was underscored in testimony in the stage 2 public hearings before PIFI.

One important example of such a fusion product was examined by the Inquiry: the IAS "special report" on "China's foreign interference activities" (PCO 2022; IAS 2022). This report was also featured in the NSIRA special report on intelligence dissemination issues and was also scrutinized by PIFI and party counsel (NSIRA 2024). The special report, elements of which were leaked to the media, was one that PCO IAS believed was a significant product that deserved the attention of senior officials, ministers and the prime minister, although it did not achieve that dissemination. Green told the Inquiry that "this paper was an innovative attempt to marry the international and the domestic because there was a big debate about whether or not, particularly China, which is the subject of the paper, was it really doing a lot of foreign interference in Canada" (PIFI 2024d, 24).

There are efforts currently under way to change the governance of PCO IAS and to ensure its capability to serve the needs of the National Security Council. While PIFI did not hear detailed testimony on these governance changes, we believe four things are needed. First is that the mandate of PCO IAS needs to be made sufficiently clear and its reporting products, both daily briefs and weekly reports, understood as fusion analysis. Second, because this change involves a move away from PCO IAS's traditional focus on international reporting alone, the PCO IAS workforce will need to be recalibrated to ensure that analysts have the tools and skill sets needed to effectively integrate domestic and international security reporting. Third, PCO IAS would benefit as a fusion

5 See www.pmc.gov.au/resources/2024-independent-intelligence-review-terms-reference.

6 Ibid.

centre from secondments of experienced analysts from CSIS and the RCMP, in particular. Finally, in that light, we also believe that serious thought should be given to migrating the Integrated Terrorism Assessment Centre from CSIS to IAS, while maintaining CSIS analytical capacity represented by its intelligence analysis bureau.

To operate as an effective fusion centre, the reconfigured IAS will also need to have a system in place in which it can receive regular inputs of international security and domestic security threat reporting from other departments and agencies in the Canadian NSI community.

Recommendation 7: PIFI recommends the construction, strengthening and ongoing maintenance of an integrated intelligence fusion centre at PCO, built on the expansion of the IAS, and capable of the regular production of reports that integrate domestic and international security issues. The intelligence fusion centre will serve, under the direction of the NSIA, as a major resource for the Cabinet National Security Council.

Creation of a Centralized OSINT Unit to Bring Together Technical and Human Expertise from Across the NSI Community

OSINT is a key intelligence collection discipline. It draws from the pool of publicly available information, including information circulating on the internet, to identify, corroborate, analyze and report on relevant national security issues.

OSINT presents many advantages for an intelligence community. These include:

- relative ease of access to a vast pool of information;
- timeliness;
- value as a "first resort" intelligence collection method that can be used to direct future intelligence work using other methodologies;
- low-to-no classification markings on OSINT products, which allows for wide circulation and readership and cuts through over-classification and intelligence-sharing challenges; and
- unique insights into key threats, including foreign interference disinformation campaigns.

Alongside those advantages are challenges, including the skill sets needed for OSINT analysts, the technological tools and data science capabilities required, resource issues and the building of partnerships with private sector capabilities. On top of these issues are two that are especially pertinent to the NSI community. One is a cultural shift that is required to ensure that OSINT products get the same attention and respect as intelligence reports derived from "high-side" collection methodologies. The other concerns the importance of privacy protections and the need to ensure "social licence" for OSINT activities undertaken by any federal NSI entity.[7]

As PIFI has heard in witness testimony, PCO IAS was tasked by the NSIA to review improvements that could be made to the Canadian NSI community's OSINT capabilities. The then NSIA, Jody Thomas, told the Inquiry about the purpose of this study and described it as "sort of the A to Z on what OSINT looks like in Canada and how we should

7 See the discussion in Wark (2022, 11–15).

move forward with it" (PIFI 2024e, 71). Daniel Rogers, who served as deputy NSIA and is now appointed as the head of CSIS, added that he viewed the paper as identifying where across the NSI community OSINT activities were taking place, how better cohesion could be achieved, and whether there were future policy and legislative changes that might need to be made (ibid., 72–73). He added a cautionary note that "we will need to be conscious of legal obligations and risks as we start to emerge into…a previously less used type of intelligence" (ibid., 73).

Lead examination on this topic at PIFI did not go beyond noting that these were "complex issues, all of which are under discussion at the moment" (ibid.). This represented a missed opportunity, in our view, to further track the PCO IAS study and to deepen the discussion of OSINT benefits and challenges for the Canadian NSI system.

The Inquiry had available to it a "placemat" produced by IAS in response to the NSIA tasking: "The Future of Open Source Intelligence (OSINT) in the Canadian Intelligence Community," dated April 2023 (Wark 2024a; IAS 2023). The placemat identified the value of OSINT and indicated that four pillars of study had been constructed on "Process," "Authorities," "People" and "Tools & Technology." According to the placemat, interdepartmental expert groups were to be established to examine each of these pillars, with briefings to be undertaken in June 2024 before the ADM- and deputy-minister-level committees. What the status of this work to June 2024 might be was not further examined at PIFI.

We believe that the commissioner should advance as a recommendation that a centralized, stand-alone OSINT centre of expertise should be created with a dual mission: to coordinate and bring coherence to the various mandated activities in the OSINT field across the NSI community; and to serve as a principal resource for strategic OSINT reporting, fusing domestic and international reporting. To be effective, the OSINT centre would need sufficient human resources, budget, technological capacities and authority to create external partnerships. It would need a clear, Charter of Rights and Freedoms-compliant mandate, and there would have to be a public explanation of its work, to assist in generating social licence. A public annual report on its activities should be generated. Consideration would also have to be given to establishing the OSINT centre through legislation.

Recommendation 8: The government should create an OSINT centre of expertise with appropriate mandate and authorities.

Strengthening of the Federal Government's Capacity to Detect and Report on Foreign Interference Disinformation Campaigns

Foreign interference in Canada's digital information environment and the conduct of foreign interference-related disinformation campaigns must be flagged as a key concern. As a "non-traditional" means of foreign interference, it should be considered one of the emerging and most significant threats to our democratic processes. Making recommendations to "detect, deter and counter" disinformation is central to the Commission's work.

The Inquiry has heard a considerable amount about the role of RRM Canada and its disinformation tracking, analysis and reporting. The RRM currently plays a unique role in the NSI community as a centre of expertise on foreign disinformation campaigns operating in Canada's information space. In our view, it cannot continue to shoulder that burden as presently constituted.

The RRM was created following the 2018 Group of Seven (G7) meeting to perform a coordination function to respond to a variety of shared threats to democracy. It was only after the Russian invasion of Ukraine that the prime minister announced, in August 2022, the establishment of a dedicated unit within RRM Canada at GAC to address foreign state-sponsored disinformation. The emphasis at the time was on Russian disinformation campaigns in light of the Russian invasion of Ukraine.[8]

RRM Canada's disinformation unit is still in its formative phase, its resources are miniscule, and its capacity to engage with a range of expert private sector media monitoring and OSINT organizations is very limited. It was an innovative idea and has great potential, but its engine room is far too small and its fit, as a GAC unit within the broader Canadian NSI community, is problematic.

The experiment that was RRM Canada now needs to be continued on a more secure foundation. To serve as an effective centre for the detection of foreign state actor disinformation campaigns targeting Canada, a number of changes must be made. These fall under two directions: governance and resources.

On governance, RRM Canada should be relocated from GAC to either Public Safety or PCO. Placement at Public Safety would allow a reconstituted RRM Canada to work with the NCFIC's office, offering a potentially effective synergy. Being situated at either Public Safety or PCO would allow for better convening power for RRM Canada across the NSI community and better coordination of effort.

RRM Canada will also need a clear mandate, including governance rules around making public attributions of foreign state-sponsored disinformation campaigns. Wherever its new home may be, RRM Canada should continue to play a key role in the SITE Task Force.

To stay true to its original mission as a coordination mechanism for the G7 in responding to threats to democracy, a small secretariat with an international cooperation mandate — and to serve as Canada's focal point — should continue to operate from within GAC.

As for resources, it is not enough to say that RRM Canada simply needs more, as true as that is. What RRM needs are the right human and technological resources. There are distinctive skill sets associated with RRM Canada's work, including diverse linguistic skills, data science capabilities, geopolitical knowledge and understanding of the Canadian information environment. Talent spotting may be difficult, retention may be challenging and training will be a constant requirement. In addition, RRM Canada needs access to the right technological tools to monitor social media platforms in particular.

Finally, RRM Canada will need the capacity to work in partnership with private sector and academic institutions devoted to various forms of media monitoring.

In light of all of the above, the budget for a reconstituted RRM Canada will need to be considerably expanded to secure a professional workforce, the technological tools it will require, and the partnerships and networks it must develop.

Recommendation 9: PIFI should support the relocation of the foreign disinformation tracking unit (RRM Canada) from GAC to Public Safety or to PCO. RRM Canada needs a clear mandate, including for public attribution of foreign state information operations, and much greater resources.

8 See www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/index.aspx?lang=eng; GAC (2022).

Re-imagining the Role of the NCFIC

Detecting, deterring and countering foreign interference requires a whole-of-government response involving the contributions of many departments and agencies, in accordance with their authorities.

NSICOP grasped this reality in its first study of foreign interference, issued as part of its 2019 annual report. It commented on the ad hoc and case-specific nature of responses to foreign interference and recommended "whole-of-government operational and policy mechanisms" (NSICOP 2020, 109). NSICOP also called attention to the mandate of the Australian national counter foreign interference coordinator and suggested it as a possible model for Canadian practice (ibid.).

The Canadian government eventually adopted this recommendation, announced by the prime minister as one measure to tackle foreign interference, in a statement issued in March 2023 (Prime Minister of Canada 2023).

The NCFIC is an ADM-level official at Public Safety who is double-hatted in a role with the National and Cyber Security Branch. The NCFIC is meant to serve as the Public Safety department's lead on foreign interference issues and to play a coordinating role within the wider NSI community. In addition, the NCFIC has also taken on a recent outreach function with Parliament and diaspora communities.

In essence, the new NCFIC is filling policy, coordination and outreach vacuums and attempting to do so with a very small staff. It could be said that the government is doing foreign interference coordination and outreach "on the cheap." The terms of reference for the NCFIC demonstrate a significant mismatch between the office's resources and the scope of its mission (Public Safety Canada, n.d.). We also believe that the NCFIC mandate, as presently constituted, is too minimalist when it comes to engagement with non-federal stakeholders (ibid.). NCFIC does not even have a public-facing website.

In our view, the NCFIC function needs to be strengthened before its ad hoc work overwhelms it. It needs a higher profile within government, requires more resources, and needs direct connectivity to disinformation-tracking intelligence units and assessment fusion centres.

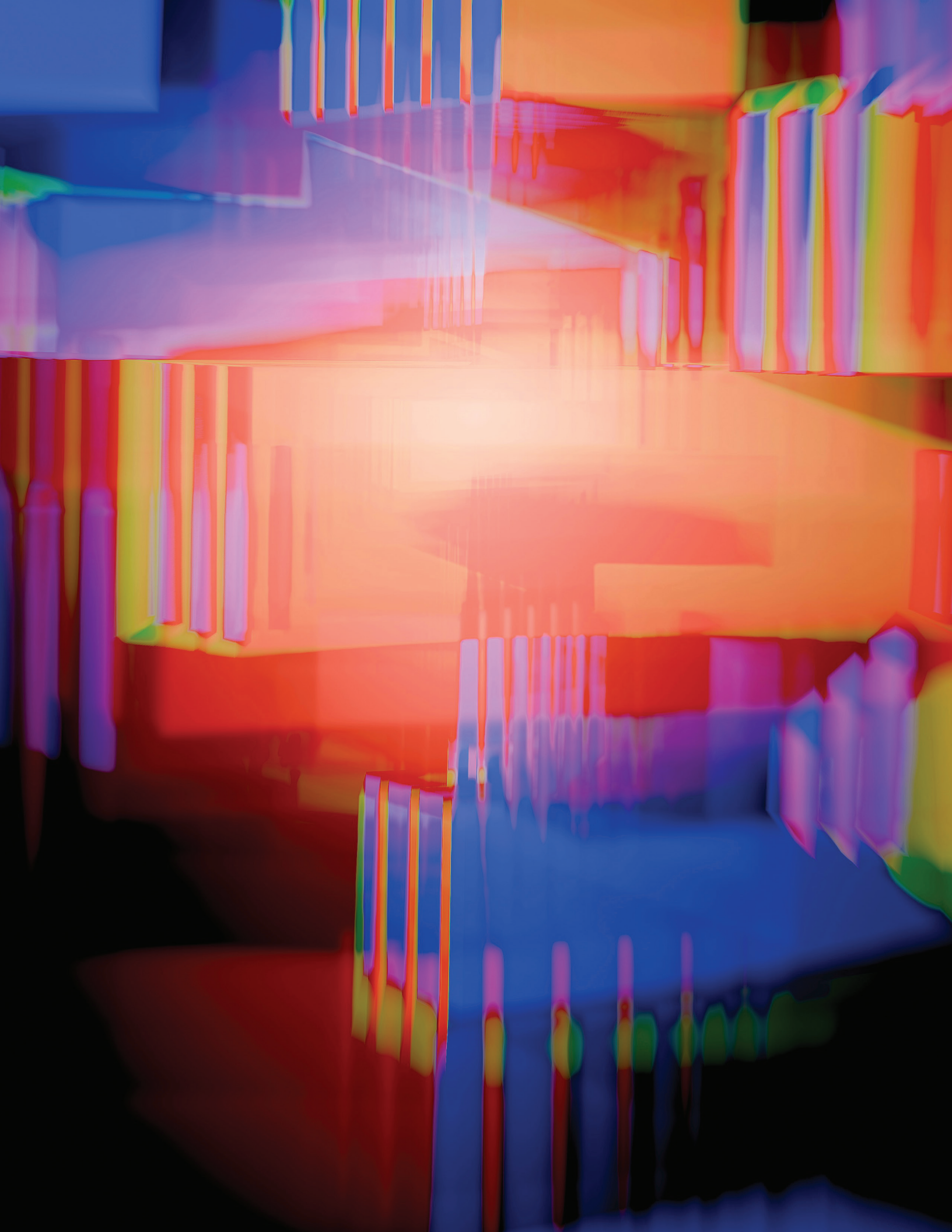
We also believe that it must take on both a coordination and operational role in terms of public and parliamentary outreach on foreign interference issues.

It will take not just additional resources to fulfill an expanded mandate but also time. That time should be used, in our estimation, to more fully consider allied models that combine internal coordination and public outreach, including the Australian counter foreign interference coordinator and the Swedish Psychological Defence Agency, to gauge best practices.[9]

Ultimately, the NCFIC should become both an internal and a public-facing centre of excellence on foreign interference, with a capacity to generate research projects and important public education products.

Recommendation 10: PIFI should recommend that the new NCFIC office be strengthened, provided with additional resources, be fully connected to intelligence reporting, and develop a coherent strategic plan for public outreach, education and parliamentary engagement.

9 See websites for the Swedish Psychological Defence Agency at https://mpf.se/psychological-defence-agency and for the Australian counter foreign interference coordinator at www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/.



Intelligence Dissemination Challenges and Reforms

There are many definitions of intelligence. Perhaps the most concise and elegant is that offered by Sir David Omand: "The most basic purpose of intelligence is to improve the quality of decision-making by reducing ignorance" (Omand 2010, 22). To fulfill that purpose, relevant high-quality intelligence must be able to reach decision makers in a timely way, hence the importance of intelligence dissemination.

Significant problems with intelligence dissemination were noted in the first report by David Johnston, the appointed independent special rapporteur, and were featured in a special report from NSIRA. Testimony and records provided to PIFI have further illustrated problems with intelligence dissemination, as well as indicating that some significant changes have been made to improve the flow of intelligence to decision makers, particularly through the expanded use of CSE systems and client relations officer document delivery, and to ensure a capacity for tracking. Less has been said about any system capture of the response by intelligence consumers of intelligence products. Green's testimony might be noted in that regard. He commented, perhaps somewhat obliquely:

> It [intelligence] is tracked and, you know, who has access to it, and in a lot of cases who's being briefed on it. There is a nuance I think with respect, you know, there's a tremendous amount of material. So, I don't think it tracks that, you know, an individual briefing was, you know, fully absorbed. There's a nuance in there that I think is important. You know, you can know who saw it, and who read it, or who was briefed on it. I think there is a bit of a difference with respect to has that actually been, sort of, absorbed at a certain level? Because there's an awful lot of material. (PIFI 2024d, 22)

We would like to put a finer point on this observation by noting that a reformed intelligence dissemination machinery is incomplete without a feedback mechanism to record, in some way, responses to intelligence reports by consumers. Tracked responses could include comments on reports, critiques, or requests for additional information or follow-up briefings.

PIFI has heard testimony in stage 2 of the public hearings from officials about new intelligence dissemination and tracking mechanisms. Only the Commission is in a position, given its access to classified reporting, to decide whether there is yet sufficient evidence to assess the effectiveness of the changes that have been made.

Where we believe we can add a useful voice is regarding the functions of the NSIA to the prime minister. The NSIA plays a critical role in intelligence dissemination to senior officials through the new Deputy Minister Committee on Intelligence Response and to the prime minister and Cabinet, and especially to the National Security Council, for which the NSIA serves as secretary.

More broadly, the role of the NSIA is two-fold: to ensure coordination of the NSI community; and to advise the prime minister on relevant NSI issues needing their attention. To these should be added an international liaison role with counterpart officials from the Five Eyes and other countries.

The responsibilities of the office are extremely onerous: the flow of intelligence reports is vast; coordinating a decentralized and siloed NSI community is hard work; and

international travel is demanding. In particular, the challenge of serving as an important gatekeeper for intelligence dissemination to senior officials and ministers cannot be understated.

To ensure the effective functioning of the NSIA, we believe the following measures would be of assistance:

- An ideal candidate "profile" for the NSIA should be maintained by the clerk of the PCO, supported by official "leaving" interviews conducted with previous NSIAs.
- A "mandate-"style letter should be provided to the NSIA by the prime minister and, as with ministerial mandate letters, be made public.
- The NSIA role should be a singular function, not combined with any other duties at PCO.
- The NSIA should be supported by a deputy.
- The NSIA office requires more staff resources.
- Decisions on intelligence dissemination to deputy heads and ministers should be recorded, with their rationales.

We appreciate that NSICOP is engaged in its own study of the NSIA function and will report after the PIFI produces its final report. Nevertheless, we believe it important for the Inquiry to make its own recommendations on the NSIA role.

Recommendation 11: PIFI should emphasize the importance of the role of the NSIA and recommend strengthening the function with several measures, including creating a profile for the office holder and having the prime minister provide the NSIA with a mandate letter. The recent provision of a mandate letter should be regarded as a standard practice going forward. A stronger secretariat capacity at PCO is required for the NSIA to perform a coordination role for the NSIA community, be a key disseminator of intelligence to the prime minister and Cabinet, and function as the top representative of the Canadian NSI community with Five Eyes partners and others.

The Role of the RCMP

The RCMP is Canada's national police force and has a mandate to investigate and lay charges regarding national security offences under the Criminal Code. This mandate did not change with the creation of CSIS in 1984, but the duality of having a law enforcement agency and a civilian security service without police powers operating in the national security space has required the two entities to seek and refine ways to cooperate and share intelligence (the "one vision" doctrine) and has given rise to the long-lasting and much discussed "intelligence to evidence" problem as it pertains to prosecution of crimes.

The RCMP is guided by the mantra of "intelligence-led" policing and was encouraged by the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar in recommendation 1 of its 2006 final report to continue to upgrade its intelligence capabilities. An RCMP document titled "RCMP Federal Policing: Ideologically Motivated Violent Extremism (IMVE) Strategy," from April 2024, recently released in an access to information and privacy request, notes that the force's "intelligence mandate is currently being underutilized due to significant resourcing constraints and internal uncertainties

and misconceptions about the permissible scope of FP [federal policing] duties and authorities in the intelligence context" (Thompson 2024, 19).

This internal finding has been replicated in other recent reports. One was a lessons-learned exercise following the Freedom Convoy protests, code-named "Natterjack." It involved two components: a questionnaire provided to all RCMP members involved in the national response to the Freedom Convoy protests; and an analysis of the responses to the questionnaire and recommendations offered by a retired RCMP assistant commissioner. One of the four key themes of Project Natterjack involved intelligence sharing. The report noted multiple problems with the RCMP's use of intelligence during the Freedom Convoy protests and, among other things, recommended the creation of a "major event" intelligence unit at national headquarters. Whether that recommendation was taken up is not known. It could have important implications for the RCMP's ability to deal with a range of national security threats, including foreign interference (Wark 2022, 2024b).

NSICOP undertook a major study of the federal policing mandate of the RCMP and issued a (redacted) special report in November 2023. One of its key findings was directed at the minister of public safety, encouraging the minister to "take a greater role with respect to issues such as governance, priorities, and organizational direction" (NSICOP 2023, 85). It noted that the RCMP "cannot effect the necessary changes alone" (ibid.). In its recommendations, NSICOP called on the government to provide adequate resources to the RCMP to fulfill its federal policing mandate (ibid.).

Media reporting indicates that Minister of Public Safety Dominic LeBlanc had written to provincial counterparts in the spring of 2024 to indicate that the government plans to give federal policing more capacity to engage in major investigations, including in foreign interference, while not envisioning a federal policing force completely separated from contract policing (Hager and Freeze 2024).

The ability of the RCMP to operationalize intelligence-led policing is critical to its contribution to detecting, deterring and countering foreign interference, whether through prosecutions or other means such as threat reduction or outreach. This criticality has been heightened by new provisions contained in Bill C-70, especially regarding amendments to the Foreign Interference and Security of Information Act.[10]

Clearly, reforms to the RCMP's national security capabilities to deal with foreign interference threats, among others, are required, and the matter is under active consideration internally. None of the studies cited above were led by Commission counsel in their examination of senior RCMP officials as part of the stage 2 public hearings on October 3, 2024.

What contribution, then, might PIFI make in its final report?

In our view, PIFI can best assist by taking the NSICOP report one step further and recommending that the minister of public safety prepare and publish a concrete strategic plan for the reform of RCMP federal policing. This plan should be shared with other levels of government and the Canadian public. Consideration might also be given to the idea of circulating a "green" paper for public discussion on issues to do with reform of the RCMP. These recommendations might well fall to a future government to implement but should be advanced all the same.

Recommendation 12: PIFI should recommend that the minister of public safety develop and publish a strategic plan for reform of RCMP federal policing to ensure that it can be effective in dealing with foreign interference threats in the future.

10 Bill C-70, *An Act respecting countering foreign interference*, 1st Sess, 44th Parl, 2024 (assented to 20 June 2024, s 54 amending s 20 of the *Security of Information Act*), online: <www.parl.ca/Content/Bills/441/Government/C-70/C-70_4/C-70_4.PDF>.

Adjudicating the NSICOP Special Report on Foreign Interference

NSICOP issued a controversial *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions* in June 2024. It was tabled in Parliament in redacted form a month after the publication of the PIFI initial report.

The NSICOP report contained serious allegations regarding the complicity of parliamentarians in foreign interference campaigns. It noted that foreign state actors deployed traditional (human-to-human) means, "establishing reciprocal relationships with influential Canadians, using clandestine networks, employing proxies, and covertly buying influence with candidates and elected officials" (NSICOP 2024, 24). The NSICOP report went on to say: "In the period under review, CSIS and CSE produced a body of intelligence that showed that foreign actors used deceptive or clandestine methods to cultivate relationships with Canadians who they believed would be useful in advancing their interests — particularly members of Parliament and senators — with a view to having the Canadian act in favour of the foreign actor and against Canada's interests" (ibid.).

The details of the allegations contained in the NSICOP report, including in highlighted case studies, are heavily redacted in the released version of the report.

Two leaders of opposition parties in the House of Commons obtained top secret (TS) clearances in order to read the classified version of the report. They both made public statements that contained diametrically opposed perceptions of the contents of the report. The leader of the Bloc Québécois is apparently still in the process of obtaining his clearance. The leader of the Conservative Party of Canada refused to obtain a security clearance and thus is unable to read the classified report.

The publication of the NSICOP report has produced an understandable and heated furor. Its effect, to date, has been to undermine trust in Parliament and parliamentarians and to sow considerable confusion in public about the nature and significance of the allegations. There has been constant pressure within Parliament, in the media and in public discourse for the government to "name names" of parliamentary foreign interference accomplices, no matter how much such a process might offend principles of natural justice, the rule of law and democratic processes. This pressure has extended to a suggestion that PIFI should "name names" in its final report. We commend the commissioner for refusing to do any such thing.

In response to a House of Commons motion of June 11, 2024, the commissioner committed the Inquiry to undertaking a further examination of the allegations contained in the NSICOP special report (PIFI 2024f, 2024g).

In order to conduct this examination, the Inquiry asked CSIS to review its holdings and cast further light on these allegations. As CSIS witnesses testified in the stage 2 public hearings, they engaged in a "reverse-engineering" process to unearth the intelligence reports on which the NSICOP independently drew its conclusions (PIFI 2024h). CSIS (2024) ultimately produced, in response to the Inquiry, a list of six incidents of foreign interference targeting parliamentarians over the period from 2018 to the present. The Inquiry also heard testimony from ministers, including the prime minister, suggesting that NSICOP had over-reached with its allegations.

This leaves the commissioner with a crucial and difficult task at hand in her final report. The commissioner must produce a compelling factual, evidence-based analysis of the nature and significance of the allegations concerning parliamentarians acting as

accomplices in foreign interference claims. This analysis should be accompanied by an assessment of Parliament's vulnerabilities to future foreign interference campaigns and recommendations on how parliamentarians can better equip themselves to deal with foreign interference efforts that might target them or their staff.

The commissioner's analysis of the allegations contained in the NSICOP special report can also be broadened to reflect the overall findings and recommendations contained in the report.

Only the commissioner can produce such an independent analysis, based on the Inquiry's unique access to classified records. It constitutes the Commission's most important task, and it is vital to restoring public trust and confidence in Parliament and in the federal government.

Recommendation 13: CIGI commends the Inquiry for undertaking an independent examination of the NSICOP report on foreign interference and for standing on appropriate principles to refuse to "name names." CIGI recommends that PIFI include a substantive, compelling analysis, using a "write to release" approach, of the allegations contained in the NSICOP report, and that its analysis be referred to relevant standing committees in the House (SECU and PROC) and Senate (the Committee on National Security and Defence) as well as to NSICOP, for further study.

Political Actor Literacy on Foreign Interference and National Security Threats

PIFI was established in response to opposition party pressure in the House of Commons that rejected the approach of the independent special rapporteur and insisted on a public inquiry as the only way to establish the truth about foreign interference targeting Canadian elections. The terms of reference for the Inquiry were established following closed-door negotiations between the opposition parties and the governing party. The focus of opposition party concerns, in keeping with their responsibility to hold the government to account, was the alleged failure of the government to take foreign interference seriously and to act accordingly.

What was potentially lost in this approach was the responsibility of parliamentarians themselves to be aware of foreign interference threats and to be part of an effort to enhance societal resilience across the board. What is needed, in our view, is both an enhanced ability on the part of the government to inform parliamentarians of foreign interference and other national security threats, and an enhanced capacity of parliamentarians to take steps to inform themselves. A better-informed Parliament is better able to hold the government to account, to convey its views to constituents and the Canadian public, and to defend itself and be resilient in the face of what are bound to be persistent threats — even if the manner of their delivery, whether traditional or digital in nature, may change over time.

There are a variety of steps that may be contemplated to achieve the twin objectives of greater government information sharing with parliamentarians of all parties and enhanced knowledge of parliamentarians of foreign interference and other national security threats. Some represent very low-hanging fruit.

In the category of easy to achieve, we would include the following:

- Encourage parliamentarians and their staffs to take advantage of the enormous quantity of publicly available information on foreign interference. This would require parliamentarians to take seriously threats to our national security and to become better educated about them. They can seek the assistance of their own staffs, reach out to outside experts and call on Library of Parliament staff to assist them. We would encourage party appointments to key standing committees of the House that routinely deal with national security issues to be based on a demonstrated willingness on the part of members of Parliament (MPs) to embrace education about such issues. A similar approach should animate the Senate.
- We encourage all parties to support NSICOP's work and pay close attention to its reports.
- Every party should, as federal elections approach, strengthen their campaign platforms to ensure that they demonstrate the party's commitment and approach to dealing with foreign interference and the wider range of national security threats.
- All newly elected MPs and newly appointed senators should be given a strategic briefing on national security and foreign interference threats by security and intelligence officials upon taking up their duties.
- More specialized briefings on aspects of national security threats, including cyber and physical threats, should be delivered to all parliamentarians by security officials on a regular basis.
- Party caucuses should routinely devote attention to a discussion of national security threats.
- Party leaders should make clear their party's policies on national security issues in and outside of election periods.

A step beyond (but not too far beyond) the easily achievable, is the following.

All leaders of political parties in the House of Commons should acquire a TS clearance to be briefed by senior officials from the NSI community as needed or as requested. The rationale for this is three-fold. First, a TS clearance is the best way to allow for substantive briefings on national security and foreign interference threats. Second, possession by a party leader of a TS clearance gives that leader a much better opportunity to manage risks, especially of foreign interference, on the part of their caucuses. Third, and perhaps most importantly, a TS clearance creates for an opposition leader a clear path to a better understanding of foreign interference and other threats, so that they can better position their party's policy and speak to Canadians with authority. It is, to be clear, the opposite of a gag order. Pressing into service the CSIS threat reduction measures mandate to gain knowledge of foreign interference threats, a mandate that dates back in its original form to legislation passed in 2015, while useful in specific instances of threat, is not a real alternative.

The SITE Task Force has emerged as a key mechanism for informing parties of election interference threats during the writ period. We believe that the SITE Task Force mandate should operate to cover by-elections, and that the task force should remain in operation and be vigilant between elections. It must find enhanced ways to substantively communicate knowledge of foreign interference threats, based on intelligence holdings from across the NSI community, with security-cleared party representatives. For their part, security-cleared party representatives must take the SITE Task Force opportunity for information sharing seriously.

The SITE Task Force must evolve as an intelligence fusion centre serving the NSI community, the Panel of Five, and security-cleared party representatives so that it can track a fast-changing security threat environment. In particular, the SITE Task Force must devote more attention to the rise of physical security threats to politicians and their staffs, including whether such threats may have a link to foreign interference, and continue to be able to draw upon RRM Canada for analysis of foreign state actor disinformation campaigns.

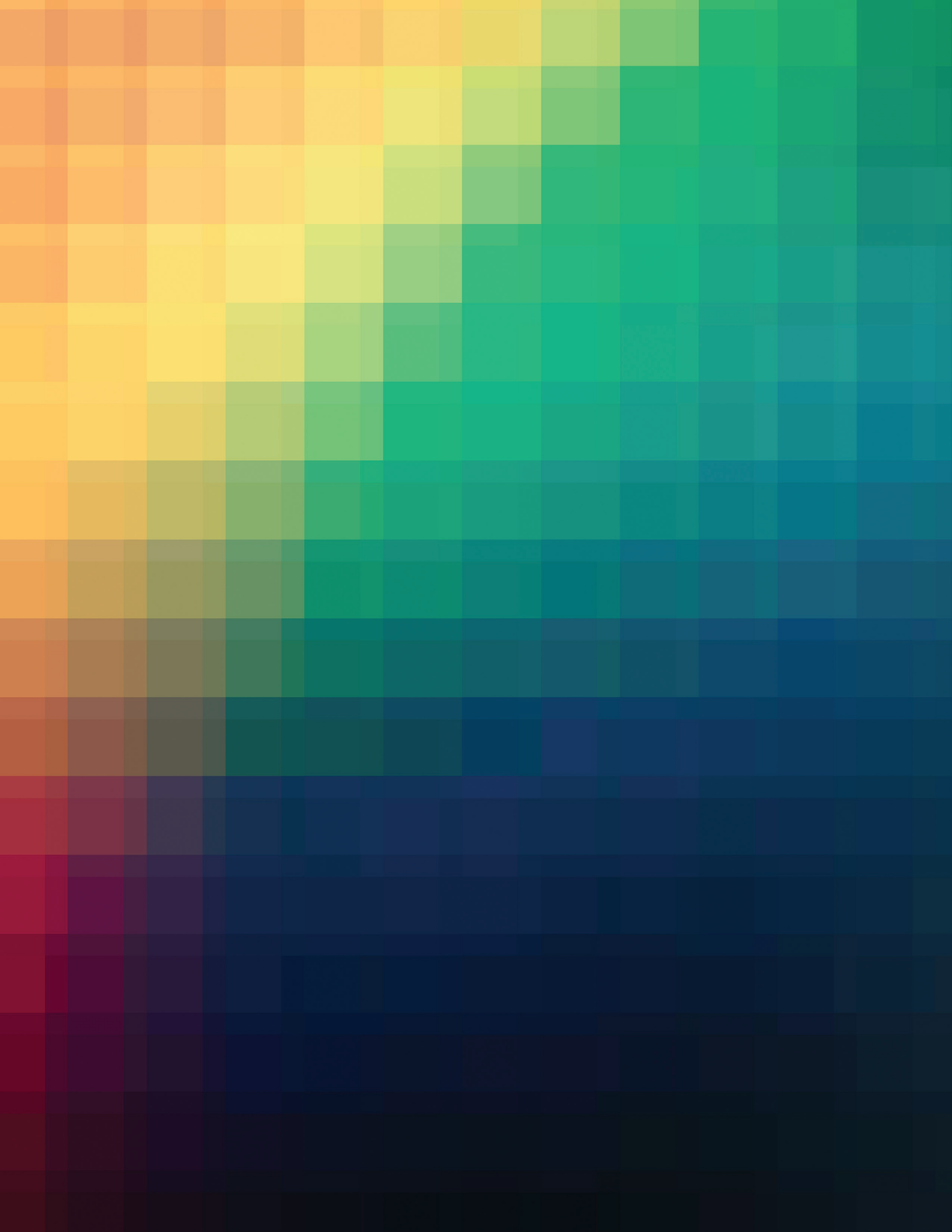
We also believe that Parliament should, wherever possible, fast-track significant pieces of national security legislation. The rapid passage of Bill C-70 was an extraordinary development and not always to be emulated, but a better time frame than the two years (2017–2019) that it took to pass Bill C-59 is needed. In considering national security legislation, Parliament should be encouraged to seek out both officials and ministers' testimony, and expert views, drawn from a wide range of perspectives. The temptation to stack witness lists with partisan voices should be avoided. Wherever possible, and especially at Committee, a non-partisan approach should be taken to national security issues.

The parliamentary intern program should include training opportunities to educate interns on national security issues. Similarly, Parliament Hill staff should have access to education and training opportunities to deepen their understanding of national security issues. CIGI has recently launched a "lunch and learn" series for Parliament Hill staff from all parties and Senate groups to advance such opportunities.

As indicated above, we believe that Parliament should support and pay attention to the reports issued on its behalf by NSICOP. It is equally important for Parliament to be able to craft revised statutes for NSICOP and NSIRA as deemed appropriate, based on experience since 2017 (for NSICOP) and 2019 (for NSIRA). The much-delayed statutory review of the acts governing both NSICOP (Bill C-22) and NSIRA (Bill C-59) should be immediately undertaken by Parliament.

Finally, in the spirit of providing parliamentarians with better educational opportunities regarding foreign interference and other national security threats, and as a complement to regular security briefing and TS clearances for party leaders, we believe that a budget should be allocated by Parliament to all recognized political parties in the House and groups in the Senate to allow them each to hire and maintain a dedicated security-cleared officer to act as an expert and trusted resource on foreign interference and, more broadly, national security threats.

Recommendation 14: CIGI suggests that PIFI recommend in its final report a series of steps to improve Parliament's ability to understand foreign interference and other national security steps. In particular, we recommend that the SITE Task Force establish an enhanced ability to share meaningful classified intelligence with security-cleared members of the parties during the writ period and that the SITE Task Force after-action report following a general election be declassified and published. We recommend that the commissioner include a strong recommendation in her final report urging Parliament to proceed, as a matter of urgency, to accomplish the delayed statutory reviews of the legislation that governs the activities of the key independent review bodies, NSICOP and NSIRA. Finally, the commissioner should recommend that a budget be allocated by Parliament to all recognized political parties in the House and groups in the Senate to allow them to hire and maintain a dedicated security-cleared officer to act as an internal expert party resource on foreign interference and, more broadly, national security threats.



Works Cited

CSIS. 2024. *Canadian Security Intelligence Service Stage 2 Institutional Report.* CAN.DOC.000044. https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Exhibits_and_Presentations/Exhibits/CAN.DOC.000044.pdf.

Department of National Defence. 2024. *Our North, Strong and Free: A Renewed Vision for Canada's Defence.* Ottawa, ON: Department of National Defence. www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html.

Fyffe, Greg. 2021. *Prepared: Canadian Intelligence for the Dangerous Decades.* Reimagining a Canadian National Security Strategy Report No. 6. Waterloo, ON: CIGI. www.cigionline.org/publications/prepared-canadian-intelligence-for-the-dangerous-decades/.

GAC. 2022. *G7 Rapid Response Mechanism: Protecting Democracy*. Annual Report 2022. Ottawa, ON: GAC. www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/2022-annual-report-rapport-annuel.aspx?lang=eng.

Government of Canada. 2024. *Canada's Intelligence Priorities.* September. Ottawa, ON: PCO. www.canada.ca/en/privy-council/services/publications/canada-intelligence-priorities.html.

Hagar, Mike and Colin Freeze. 2024. "RCMP has no plans to split itself in two to ensure more focus on terrorism, foreign interference, says public safety minister." *The Globe and Mail*, June 13. www.theglobeandmail.com/canada/article-rcmp-has-no-plans-to-split-itself-in-two-to-ensure-more-focus-on/.

IAS. 2022. *China's Foreign Interference Activities.* Special Report. January. CAN003787_RO1. https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Exhibits_and_Presentations/Exhibits/CAN003787_R01.pdf.

———. 2023. "The Future of Open Source Intelligence (OSINT) in the Canadian Intelligence Community." April. CAN027789_0001. https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Exhibits_and_Presentations/Exhibits/CAN027789_0001.pdf.

New Zealand Security Intelligence Service. 2024. *New Zealand's Security Threat Environment: An assessment by the New Zealand Security Intelligence Service.* Wellington, NZ: New Zealand Security Intelligence Service. www.nzsis.govt.nz/assets/NZSIS-Documents/New-Zealands-Security-Threat-Environment-2024.pdf.

NSICOP. 2020. *Annual Report 2019*. Ottawa, ON: NSICOP. www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_en.pdf.

———. 2023. *Special Report on the Federal Policing Mandate of the Royal Canadian Mounted Police.* August 14. Ottawa, ON: NSICOP. www.nsicop-cpsnr.ca/reports/rp-2023-11-fp/RCMP_FP_report_EN.pdf.

———. 2024. *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions.* June 3. Ottawa, ON: NSICOP. www.nsicop-cpsnr.ca/reports/rp-2024-06-03/intro-en.html.

NSIRA. 2024. *Review of the dissemination of intelligence on People's Republic of China political foreign interference,* 2018–2023. NSIRA Special Report. May 28. Ottawa, ON: NSIRA. https://nsira-ossnr.gc.ca/en/reviews/ongoing-and-completed-reviews/completed-reviews/review-of-the-dissemination-of-intelligence-on-peoples-republic-of-china-political-foreign-interference-2018-2023/.

Office of the Director of National Intelligence. 2024. *Annual Threat Assessment of the U.S. Intelligence Community*. February 5. Washington, DC: Office of the Director of National Intelligence. www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.

Omand, David. 2010. *Securing the State*. New York, NY: Columbia University Press.

PCO. 2022. "IAS Report on China's Foreign Interference Activities." January 20. CAN011049_0001. https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Exhibits_and_Presentations/Exhibits/CAN011049_0001.pdf.

PIFI. 2020. "Canada's Strategy for Countering Hostile Activities by State Actors." September 2. Version 9. CAN003249. https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Exhibits_and_Presentations/Exhibits/CAN003249.pdf.

———. 2024a. *Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions — Initial Report*. May 3. https://foreigninterferencecommission.ca/fileadmin/user_upload/Foreign_Interference_Commission_-_Initial_Report__May_2024__-_Digital.pdf.

———. 2024b. *Decision on Applications for Standing*. December 4. https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Procedural_Documents/Decisions/decision_on_standing_dec_04_2024.pdf.

———. 2024c. *Public Hearing*. Volume 38. October 23. https://foreigninterferencecommission.ca/fileadmin/user_upload/PIFI_-_Public_Hearings_-_Volume_38_-_October_23__2024-English_Interpretation.pdf.

———. 2024d. *Public Hearing*. Volume 29. October 7. https://foreigninterferencecommission.ca/fileadmin/user_upload/PIFI_-_Public_Hearings_-_Volume_29_-_October_7__2024-English_Interpretation.pdf.

———. 2024e. *Public Hearing*. Volume 31. October 9. https://foreigninterferencecommission.ca/fileadmin/user_upload/PIFI_-_Public_Hearings_-_Volume_31_-_October_9_2024-English_Interpretation.pdf.

———. 2024f. "5th Notice to the Public." August 29. https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Procedural_Documents/Notices/2024-08-29_-_5th_Notice_to_the_Public.pdf.

———. 2024g. "4th Notice to the Public." June 17. https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Procedural_Documents/Notices/Fourth_Notice_to_Public_June_17_2024_FINAL.pdf.

———. 2024h. *Public Hearing*. Volume 24. September 27. https://foreigninterferencecommission.ca/fileadmin/user_upload/PIFI_-_Public_Hearings_-_Volume_24_-_September_27__2024-English_Interpretation.pdf.

Prime Minister of Canada. 2023. "Taking further action on foreign interference and strengthening confidence in our democracy." News release, March 6. www.pm.gc.ca/en/news/news-releases/2023/03/06/taking-further-action-foreign-interference-and-strengthening.

Public Safety Canada. n.d. "Office of the National Counter-Foreign Interference Coordinator (ONCFIC): Terms of Reference." Memorandum for the Deputy Minister. File No. PS-042408. https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Exhibits_and_Presentations/Exhibits/CAN044981_R01_0001.pdf.

Thompson, Elizabeth. 2024. "RCMP plans to go undercover online to trap violent extremists." CBC News, November 3. www.cbc.ca/news/politics/violent-extremism-online-surveillance-1.7371494.

Wark, Wesley. 2022. "Commissioned Paper: The Role of Intelligence in Public Order Emergencies." Research paper prepared for the Public Order Emergency Commission, August–September. https://publicorderemergencycommission.ca/files/documents/Policy-Papers/The-Role-of-Intelligence-in-Public-Order-Emergencies-Wark.pdf.

———. 2024a. “Where is Canadian OSINT? Its complicated, says a senior official.” Wesley Wark’s National Security and Intelligence Newsletter, October 21. https://wesleywark.substack.com/p/where-is-canadian-osint.

———. 2024b. “A Natterjack sighting! Or, the RCMP questions itself after the Freedom Convoy.” Wesley Wark’s National Security and Intelligence Newsletter, March 29. https://wesleywark.substack.com/p/a-natterjack-sighting.

CIGI

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org