Protecting Canada Against Harm from Foes: Navigating Insider Economic-Based Threats to National Security in Critical Infrastructure with Bill C-26

By
Courtney Aucoin

Drafted April 2024

Table of Contents

Canada's Open for Business: Attracting Investment & Foreign Interference in Critical Sectors

Currently, foreign interference is one of the greatest strategic threats to Canada's national security ("NS").[1] As a host country for advanced research & development and profitable investment opportunities, Canada's critical infrastructure ("CI") remains a high-value target.[2] Foreign threat actors have leveraged human or cyber-espionage, manipulation of imports and exports, exploitation of licenses and rights, and other covert tactics to target Canadian interests to gain an economic and geopolitical advantage.[3] These are **economic-based threats** ("EBT") to NS and can stem from the acquisition of sensitive goods (including technologies and expertise), funding partnerships with research & academic institutions, and foreign investment from hostile actors in CI that are important to Canadian security interests.[4]

EBTs and **insider threat & risk mitigation** have developed substantially as two distinctive research areas in NS literature over the last ten years. To simplify the concept of EBTs as a prevalent **foreign interference** issue, this research project proposes that by converging the two themes and looking at both camps of research findings, it can be concluded that economic security issues, as high-priority NS threats in the 21st century, are possible because threat actors gain internal access through insider EBT gateways (which will be presented subsequently). Threat actors seek access to a process, good, service, or internal relationship that will be used deceptively to gain access to a more desirable target that might be directly associated with or much further

---

[1] Public Safety Canada, "Foreign Interference" (24 November 2023), online: *Government of Canada* <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/frgn-ntrfrnc/index-en.aspx>.
[2] Public Safety Canada, "National Cross Sector Forum: 2021 – 2023 Action Plan for Critical Infrastructure" (2021), online (pdf): *Government of Canada* < https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/2021-ctn-pln-crtcl-nfrstrctr-en.pdf> at 5.
[3] Dan Ciuriak & Patricia Goff, "Economic Security and the Changing Global Economy" (2021), online (pdf): *Centre for International Governance Innovation* https://www.cigionline.org/publications/economic-security-and-the-changing-global-economy/ at 5-6.
[4] Government of Canada, "Economic-Based Threats to National Security" (11 February 2021), online: *Government of Canada* <https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/07-en.aspx>.

down the supply chain.[5] Merging the two concepts, and viewing insider EBT gateways as an overarching term to describe the entry point of origin for economic interference will help conceptually clarify this type of threat activity so that government agencies, Canadian businesses, research institutions, and beyond can use this merged concept to mitigate insider threat access. This narrower scope of foreign interference merits further consideration by NS experts at an important time when significant cybersecurity legislative developments are happening in Canada.

Canada's Bill C-26 titled "*An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*" (Bill C-26") was making its way through Parliament and was being considered by the Standing Committee on Public Safety and National Security ("Committee") at the time of writing this paper.[6] Bill C-26 includes amendments to the *Telecommunications Act* which will allow the Governor-in-Council to prohibit the use of products or services of certain suppliers in Canada's telecommunications systems sector.[7] As well, the legislation enacts the *Critical Cyber Systems Protection Act* ("*CCSPA*") "to help to protect critical cyber systems to support the continuity and security of vital services".[8] Additionally, the *CCSPA* defines "Vital Services and Vital Systems" which imposes the title of "Designated Operator" to organizations, along with elevated cybersecurity responsibilities compared to those in CI, in specific federally regulated sectors which are telecommunications services, interprovincial or international pipeline and power systems, nuclear energy systems, transportation systems that are within the legislative authority of Parliament, banking systems, and

---

[5] Canadian Centre for Cyber Security, "The cyber threat from supply chains" (20 August 2021), online (pdf): *Government of Canada* <https://www.cyber.gc.ca/sites/default/files/cyber-threat-supply-chains-v3-e.pdf> at 8.
[6] Parliament of Canada, "An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts" (Modified 10 April 2024), online: *Government of Canada <https://www.parl.ca/legisinfo/en/bill/44-1/c-26>*.
[7] *Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 1st Sess, 44th Parl, 2, 2021, art 2.
[8] *Ibid*, art 5.

clearing and settlement systems.[9] More broadly, as it will be examined forthwith, the insider EBT gateway framework will aid in evaluating how Bill C-26 can be leveraged, in the future, to proactively address foreign interference in CI.

I) Research Questions

This academic paper is based on the following research questions:

a) What insider economic-based threat gateways to national security originating from hostile states in critical infrastructure pose the greatest risk of harm to Canadian interests?

b) What policy improvements could be made to Bill C-26 to enhance Canada's legislative response to insider economic-based threats and risk mitigation originating from Hostile States in critical infrastructure?

II) Research Thesis

The first part of this academic paper will identify state threat actors that have demonstrated upward trends in foreign interference activity. The second part of the paper will propose three prominent types of insider EBT gateways in Canada that are sought after by foreign states which include internal access through foreign investment and ownership, operational relationships in supply chains, and malicious personnel in Canadian organizations. Finally, once the NS vulnerabilities have been identified, a policy modification to Bill C-26 will be proposed in the third part of this text that would likely advance Canada's legislative response to insider EBTs to ensure that hostile states are deterred from pursuing Canadian interests in the future.

[9] *Supra* note 7, ss 2, 6 and 13.

Findings & Analysis: Identifying State Threat Actors, Economic-Based Threat Gateways & Changes to Bill C-26

Part I. Identify Threat Actors

a) Hostile States

In the Canadian context, foreign interference is defined as "activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person".[10] Recently in 2023, a Canadian military document was released stating that China and Russia are Canada's main states of concern in the realm of NS due to their repeated violations of international law globally as well as their direct attacks on Canada's NS interests over the last five years.[11] For the sake of the proposed framework, a **Hostile State** is a prominent threat actor, influenced or backed in any way through state influence, that leverages covert, malign, clandestine, and deceptive means to conduct threats, harassment, or intimidation directed at Canadian communities, institutions, or organizations.[12] Therefore, for the sake of the research project, China and Russia will be considered under the broader category of 'Hostile States'.

i) The People's Republic of China

Canada continues to be targeted by foreign interference on behalf of the People's Republic of China ("PRC").[13] The Chinese government, as an authoritarian regime, seeks to leverage deceptive investments, geopolitically motivated business relations, integration of surveillance and information-gathering systems or sources (economic espionage) in supply chains, as well as secretive theft of intellectual property in the interest of becoming the world's greatest state

---

[10] *Canadian Security Intelligence Act*, RSC 1985, c C-23, s 2.
[11] David Pugliese, "Russia and China at war with Canada, says Gen. Wayne Eyre" (26 October 2023), online: *Ottawa Citizen* <https://ottawacitizen.com/news/national/defence-watch/russia-and-china-at-war-with-canada-says-gen-wayne-eyre>.
[12] Public Safety Canada, "Foreign Interference and Hostile Activities of State Actors" (20 August 2021), online: *Government of Canada* <https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/08-en.aspx>.
[13] *Ibid*.

superpower.[14] PRC-backed organizations have integrated threat actors into Canadian CI business organizations and pose a significant threat to Canadian sovereignty, NS interests, innovation and development, Canadian privacy, and commercial assets.[15]

According to experts who have testified before the Committee, it is not uncommon for Chinese firms that are engaging in commercial activities in the Canadian economy to work with their government's intelligence agencies to gain information on foreign corporations to eventually acquire important technology and innovative practices for strategic gains.[16] Annually, the PRC provides Chinese companies with a list of foreign assets that are considered desirable to the government's geopolitical interests which demonstrates the proximity of PRC influence and Chinese foreign business activity.[17] Also, with ongoing hearings to investigate alleged foreign interference by the PRC, India, and Russia in the 2019 and 2021 federal elections, it is clear that Canada recognizes the threat that the PRC poses to NS interests and that the regime is targeting Canadian citizens, businesses, and research institutions.[18]

ii) Russia

In its *2019 Annual Report*, the National Security and Intelligence Committee of Parliamentarians stated that the Russian Federation primarily conducts foreign interference by exerting political influence over the Canadian population and through sophisticated cybersecurity

---

[14] Federal Bureau of Investigation, "The China Threat" (Consulted 10 April 2024), online: *What We Investigate* <https://www.fbi.gov/investigate/counterintelligence/the-china-threat>.
[15] Royal Canadian Mounted Police, "Hydro-Québec employee charged with espionage" (24 November 2022), online: *Royal Canadian Mounted Police*, online: *Government of Canada* < https://www.rcmp-grc.gc.ca/en/news/2022/hydro-quebec-employee-charged-espionage>.
[16] House of Commons, Standing Committee on Industry, Science and Technology, *Minutes 8 June 2020*, (Evidence).
[17] *Ibid*.
[18] Catharine Tunney, "Canada a 'high-priority' target for Chinese interference, CSIS doc tells Hague inquiry" (1 February 2024), online: *CBC* <https://www.cbc.ca/news/politics/foreign-interference-inquiry-vigneault-cse-pco-1.7100577#:~:text=%22PRC%20%5Bforeign%20interference%5D%20activity,assessment%20by%20the%20Canadian%20Security>.

attacks by Russian intelligence officers to engage in threat-related activities.[19] More broadly amongst Canadian NS allies, international intelligence demonstrates that Russian cyber threat actors are exploring potential counterattacks against Canada, the United States, and other North Atlantic Treaty Organization and Five Eyes Allies in CI sectors in the future.[20] By turning to more recent case examples, Russian state-sponsored threat actors have been able to gain access to critical industrial control systems in Canadian CI to install destructive malware.[21] Due to Russia's foreign interference capabilities, attacks against Canadian sovereignty, violation of international law, and combined capabilities with the PRC, Russia is certainly a hostile threat to NS interests.

b) Emerging States

Similar to Hostile States, **Emerging Hostile States** ("Emerging States"), still demonstrate prevalent threat activity in Canada but are not yet considered Hostile States when referenced in recent communications by Canadian NS agencies or CI organizations that have been subject to previous foreign interference activity.

Iran

Arguably, Iran is one of Canada's most concerning Emerging States at risk of threatening Canadian people, institutions, and assets.[22] According to a legal expert, there are approximately 700 individuals in Canada with permanent residence or citizenship who have been identified as having ties to the Islamic Republic of Iran and since data collection is still underway, the number

---

[19] National Security and Intelligence Committee of Parliamentarians, "Chapter 2: The Government Response to Foreign Interference – Part 1 Annual Report 2019" (2019), online: *National Security and Intelligence Committee of Parliamentarians (NSICOP)* <https://nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/02-03-en.html>.
[20] Cybersecurity Advisory, "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure" (Modified 9 May 2022), online: *Cybersecurity & Infrastructure Security Agency* <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a> at 4.
[21] *Ibid*.
[22] Negar Mojtahedi & Brennan Leffler, "'Far Worse than you can imagine': How Iran's regime has 'spread its tentacles' in Canada" (11 November 2023), online: *Global News* <https://globalnews.ca/news/10076891/iran-dissidents-threats-canada/>.

of people is likely closer to 1000.[23] Furthermore, it is known that Iran has been able to exert its influence on the Canadian public.[24] Earlier this year, unsealed United States Department of Justice documents revealed that two Canadians planned to conduct assassinations in the United States on behalf of Iran's intelligence services.[25] As well, from a political standpoint, Canada is currently enforcing multiple types of sanctions against Iran such as arms embargos, asset freezes, export and import restrictions, and financing prohibitions as trade countermeasures in response to violations of international law and Canadian sovereignty.[26]

It has also been noted by NS experts that Canada's likely implication in supporting military efforts led by the United States in launching retaliatory airstrikes in Iraq and Syria this year against targets linked to Iran's Revolutionary Guards will only garner more attention from Iran and could put the state at further risk of threat to NS interests.[27]

In summary, Iran's suspected interest in pursuing foreign interference and broader NS crimes internationally should result in more stringent monitoring by Canada's national security agencies and Canadian organizations (with commercial or innovation linkages to Iran) to prevent Iran from evolving into a Hostile State.

---

[23] *Ibid.*
[24] Government of Canada, "National Strategy for Critical Infrastructure*"* (2009), online (pdf): *Government of Canada* <https://www.canada.ca/content/dam/nrcan-rncan/site/critical-minerals/Critical-minerals-strategyDec09.pdf> at 2.
[25] Alexander Panetta, "Iran allegedly hired Canadians to conduct assassinations on U.S. soil, according to indictment" (29 January 2024), online: *Radio Canada* <https://www.canada.ca/content/dam/nrcan-rncan/site/critical-minerals/Critical-minerals-strategyDec09.pdf>.
[26] Government of Canada, "Canadian Sanctions Related to Iran" (Modified 27 March 2024), online: *Government of Canada* <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/iran.aspx?lang=eng>.
[27] Christi Dabu "'Global Concern': High stakes for Canada to have role in widening U.S.-Iran conflict, experts say" (3 February 2024), online: *CTV News* <https://www.ctvnews.ca/politics/global-concern-high-stakes-for-canada-to-have-role-in-widening-u-s-iran-conflict-experts-say-1.6754630>.

Part II. Identify Threat Gateways

a) Why Critical Infrastructure?

More broadly, CI, commonly known as nationally significant infrastructure, can be broadly defined as the systems, assets, facilities, and networks that provide essential services and are necessary for NS, economic security, prosperity, health, and safety of their respective nations.[28] In Canada, CI sectors include energy and utilities, finance, food, transportation, government, information and communications technology, health, water, safety, and manufacturing.[29] When a threat actor seeks to enter vulnerability points in supply chains, they are often pursued indirectly with the targeted objective usually several process, system, investment, or innovation stages further down the line.[30] Vulnerability or access points (in this paper identified as insider EBT gateways) can present themselves at any point in the supply chain or during the life cycle of a good or service.[31] For this reason, Canadian CI entities struggle with determining insider EBT gateway and anticipated targets.[32]

Hostile States seek to eventually acquire access or control over sensitive technologies, data, and CI to advance their own military and intelligence capabilities, deprive Canada of access to economic gains, employ economic coercion against Canada, and support other intelligence operations against Canadians and Canadian interests.[33] However, EBTs and foreign interference are not just matters of concern for legislators and NS agencies, but also for commercial

---

[28] *Supra* note 24 at 2.
[29] *Supra* note 24 at 2.
[30] *Supra* note 5 at 4.
[31] S*upra* note 5 at 4.
[32] S*upra* note 5 at 4.
[33] Canadian Security Intelligence Service, "CSIS Public Report 2021" (2022), online: *Government of Canada* <https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-2021-public-report.html>.

organizations in these sectors.[34] According to the Business Council of Canada ("Council"), many corporate members invest significant capital in detecting, mitigating, and responding to threat attacks.[35] More specifically in CI sectors, the Council's members invest over $100 million per year while a sizeable group pays over $500,000 annually to mitigate risk of threat activity to commercial operations.[36] The Council also pointed to a study confirming that 30% of Canada's CI sectors are serviced by Chinese-associated or owned enterprises which raises more focused concerns on the vulnerability of access to EBTs by Hostile States.[37]

b) Three Primary Economic-Based Threat Gateways in Critical Infrastructure

i) Internal Access by Foreign Investment & Ownership

First, internal access to CI goods, services, and processes can be obtained by foreign states through investment and ownership. Since foreign direct investment ("FDI") can be injected at any stage of supply chains into sectors that are indirectly or directly linked to a good, process, service, or information related to NS interests, Canada, and many of its allies, have been forced to heighten their screening requirements for FDI that may be injurious to NS.[38] Therefore, it has become incredibly difficult to predict not only the number of investment sources from foreign jurisdictions that are involved in a CI supply chain but it is also challenging to determine whether an investment could provide foreign investors with access, through their investment or ownership relationship with a Canadian organization, to NS interests.

---

[34] Business Council of Canada, "Economic Security is National Security: The Case for an Integrated Canadian Strategy" (7 September 2023), online: *Business Council of Canada* <https://thebusinesscouncil.ca/report/economic-security-is-national-security/#:~:text=Canada%20faces%20a%20series%20of,and%20co%2Dopted%20academic%20research>.
[35] *Ibid*.
[36] *Ibid*.
[37] *Supra* note 34.
[38] Dimitri Slobodenjuk et al., "The Evolving Concept of National Security Around the World" (6 December 2023), online: *Global Competition Review* <https://globalcompetitionreview.com/guide/foreign-direct-investment-regulation-guide/third-edition/article/the-evolving-concept-of-national-security-around-the-world>.

Even in cases where the Government of Canada ("Government") orders a divestiture of a hostile state's investment in a Canadian company that may be deemed injurious to NS (for example: the recent case of the Minister of Public Safety ("Minister") who ordered three Chinese Canadian Lithium firms in Canadian mining to divest their assets), Chinese ownership stakes in Canadian companies still yield significant influence over corporate decision-making in Canadian CI sectors.[39] To use the mining sector as an example, 10 to 26% of Canada's largest mining companies have significant Chinese ownership rights.[40] Recently, Canada has even gone as far as issuing Policy Statements against any investment that has ties, direct or indirect, to a state-owned enterprise which will be presumed to be injurious to Canada's NS and will only be approved under the *Investment Canada Act* on exceptional grounds.[41]

ii) Operational Relationships in Supply Chains

While linkages between NS interests or information that may be sought for competitive advantage are easier to identify (for example, technology advancing Canadian warfare proliferation capabilities), others are not as easily discernable. Stand-alone and interconnected supply chain pipelines require the involvement of different processes, systems, facilities, technologies, networks, assets, and services requiring different funding sources, producers, distributors, and other entities or actors within Canada and abroad.[42] One issue with the complexities of critical supply chains is that in the 21st century, technology can have the potential

---

[39] Jack Mageau, "Critical Minerals Securitization and Canada's China Dilemma" (19 May 2023), online: *University of Alberta* <https://www.ualberta.ca/china-institute/research/analysis-briefs/2023/critical-minerals.html>.
[40] *Ibid*.
[41] Government of Canada, "Policy Statement on Foreign Investment Review and the Ukraine Crisis" (8 March 2022), online: *Government of Canada* <https://ised-isde.canada.ca/site/investment-canada-act/en/investment-canada-act/policy-statement-foreign-investment-review-and-ukraine-crisis>; Government of Canada, "Policy Regarding Foreign Investments from State-Owned Enterprises in Critical Minerals under the *Investment Canada Act* " (8 March 2022), online: *Government of Canada* <https://ised-isde.canada.ca/site/investment-canada-act/en/policy-regarding-foreign-investments-state-owned-enterprises-critical-minerals-under-investment>.
[42] *Ibid*.

for one purpose (civilian) or several (civilian and military).[43] The Government has long recognized the potential of this threat of **dual-use technologies** and as purchasers or actors involved in the processes of a supply chain, State Threat Actors can access these technologies through insider EBT gateways by circumventing sanction and export controls to evade scrutiny by Canadian officials.[44]

In fact, in 2017, the Financial Transaction and Reports Analysis Centre of Canada ("FINTRAC") received voluntary information from Canadian law enforcement that a Canadian electronics company was suspected of being involved in the shipping of controlled dual-use integrated circuits (illegal exports) that were being sent to intermediary jurisdictions for transshipment to Russia.[45] The information obtained by FINTRAC contributed to establishing legal merits for seeking formal indictments abroad.[46]

Furthermore, Public Safety Canada has recently given particular attention to procurement security and reiterated the Government's continued response to protecting government procurement of sensitive goods and services from State Threat Actors.[47] In 2022, the Department of National Defence was prompted to investigate past contracts awarded to a company that was affiliated with the PRC and blacklisted by the United States Federal Communications Commission.[48] However, the Chinese business acquisition of a Canadian parent company went

---

[43] Bita Afsha & Kash Khorasani, "Dual Use Technology" (October 2020), Online (PDF): *Concordia University* <https://www.concordia.ca/content/dam/ginacody/research/spnet/Documents/BriefingNotes/EmergingTech-MilitaryApp/BN-19-Emerging-technology-and-military-application-Oct2020.pdf> at 1.
[44] Financial Transactions and Reports Analysis Centre of Canada & the Financial Intelligence Unit of the Netherlands, "Joint financial intelligence advisory: illegal procurement of dual-use goods by Russian end-users" (Modified 22 March 2024), online: *Government of Canada* <https://fintrac-canafe.canada.ca/notices-avis/avs/2024-02-20-eng>.
[45] *Ibid*.
[46] *Supra* note 43.
[47] Standing Committee on Procedure and House Affairs, "Parliamentary Committee Notes: Procurement Safety" (January 31, 2023), online: *Government of Canada* <https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20230929/17-en.aspx>.
[47] *Ibid*.
[48] Aaron D'Andrea, "National Defence to probe past contracts awarded to firm now tied to China" (8 December 2022), online: *Global News* <https://globalnews.ca/news/9334471/national-defence-sinclair-technologies-canada-china/>.

undetected for nearly 5 years during which three more government contracts were awarded to the acquired Canadian company.[49] Clearly, State Threat Actors are still managing to access insider EBT gateways despite the Government's policy efforts.

The use of Chinese technologies has equally been a source of concern due to the PRC's surveillance and cyber-intrusion capabilities which have previously been able to gain access to Canadian telecommunications systems.[50] Many Canadian ally-states banned the use of Chinese-based Huawei's telecommunications equipment on security grounds shortly after these cybersecurity findings surfaced internationally.[51] Unfortunately, Canada was a lagger in protecting its telecommunications networks from access to critical systems and later implemented the same measures despite scrutiny of delays.[52] However, the proposed amendments to the *Telecommunications Act* show a turning point in strengthening Canada's response to NS concerns by prohibiting the use of products and services from certain suppliers which target operational insider EBT gateways, if compliance is properly monitored and enforced.[53] This requirement helps close the door to operational-related EBT gateways for a narrow list of CI organizations. However, as it will be examined subsequently, the door is still open to entities who are not captured by Bill C-26.

---

[49] *Ibid*.
[50] Craig Forcese & Leah West, National Security Law, 2nd ed (Toronto: Irwin Law, 2021) at 273.
[51] Catherine Tunney & Richard Raycraft, "Canada bans Chinese tech giant Huawei from 5G network" (19 May 2022), online: *CBC News* <https://www.cbc.ca/news/politics/huawei-5g-decision-1.6310839#:~:text=Canada%20bans%20Huawei%20from%20telecom%20networks%20after%20years%20of%20delay,-2%20years%20ago&text=%22This%20has%20never%20been%20about,ban%20Huawei%20from%20telecommunication%20networks>.
[52] *Ibid*.
[53] *Supra* note 7, art 15.

iii) Malicious Personnel in Canadian Organizations

The estimated cost of economic espionage to Canadian businesses is projected to be tens of billions of dollars.[54] As found under the *Security of Information Act* ("SOIA"), economic espionage constitutes the use of trade secrets for the benefit of foreign economic entities.[55] Such activities are clandestine or unlawful directed by or involving the participation of a foreign power which are used to influence policy decisions, gain economic knowledge, manipulate proprietary information, or replicate critical technologies.[56]

In November 2022, the RCMP arrested and charged Yuesheng Wang for charges under the SOIA and the *Criminal Code* for economic espionage activity after a 4-month investigation concluded that Mr. Wang was stealing trade secrets on behalf of the PRC as an employed researcher at Hydro-Québec.[57] This was the first time that an individual had been charged with economic espionage in Canada.[58]

Most recently, a previous employee at Ontario Power Generation, an integral Crown corporation responsible for electricity owned by the Ontario Government, was arrested by the RCMP for allegedly communicating safeguarded information to a foreign entity or terrorist group with the intent to put CI at risk under the *SOIA*.[59] While the end source of the safeguarded information is still unknown, the second case of economic espionage less than two years after the first historic arrest was no coincidence. Economic espionage is happening more than the public is

---

[54] *Supra* note 34.
[55] Public Safety Canada, "Foreign Interference and Canada" (24 November 2023), online: *Government of Canada* <https://www.canada.ca/en/public-safety-canada/news/2023/11/foreign-interference-and-canada.html>.
[56] *Supra* note 9.
[57] *Supra* note 15.
[58] Canadian Press, "Former Hydro-Québec employee who is accused of spying for China pleads not guilty to new charges" (6 April 2024), online: *CBC News* <https://www.cbc.ca/news/canada/montreal/former-hydro-quebec-employee-accused-spying-china-1.7165886>.
[59] Canadian Press, "Ex-Ontario Power Generation employee arrested for alleged security breach involving foreign group" (20 February 2024), online: *CBC News* <https://www.cbc.ca/news/canada/toronto/opg-employee-alleged-security-rcmp-1.7120449>.

aware and changes to the NS landscape are occurring which demand the implementation of new security programs, cybersecurity protections, insider risk management programs, and lawful private-public information-sharing capabilities amongst Canada's national security agencies and Canadian CI commercial operations.[60]

Part III. Proposed Policy Modification

Bill C-26 is a significant legislative milestone in modernizing Canadian cybersecurity and CI regulation. However, it is a starting point, not the end of the road for reducing foreign interference activity in Canada. Canada needs to leverage Bill C-26 to take a proactive approach in mitigating future economic interference efforts by Hostile States in CI sectors. However, this requires cross-collaboration amongst Canadian NS agencies, elected representatives, and the Canadian business community (as well as research institutions and innovation entities, although they fall beyond the scope of the paper).

Policy Recommendation: Expand the Scope of the *CCSPA* to Canadian Critical Infrastructure Sectors Seeking More Sophisticated Security Measures & Guidance

While the Government exclusively recognizes ten CI sectors in the Canadian economy, Bill C-26 only covers the scope of federally-regulated services and systems in finance, energy, telecommunications and transport sectors.[61] This leaves many CI organizations at risk. These entities will not be subject to the same level of regulation and guidance from federal governments and regulated entities to ensure that Designated Operators[62] can mitigate supply chain risks, have

---

[60] *Supra* note 7.
[61] Public Safety Canada, "Protecting Critical Cyber Systems" (Modified 14 June 2022), online: *Government of Canada* <https://www.canada.ca/en/public-safety-canada/news/2022/06/protecting-critical-cyber-systems.html>.
[62] Under the *CCSPA*, a "Designated Operator" is "a person, partnership or unincorporated organization that belongs to any class of operators in the Act under Schedule 2".

a process established to report cyber security incidents[63] to the Communications Security Establishment, and be required to implement a Cyber Security Program to ensure the protection and resilience of their critical cyber systems.[64]

It is recognized that CI is an evolving grouping term, and even the Critical 5 states (Australia, Canada, New Zealand, the United Kingdom, and the United States) have recognized that to be resilient, CI and systems "need to be flexible and adaptable to changing conditions, both foreseeable and unexpected, and to be able to recover rapidly from disruption".[65] Not enough has been done legislatively to arm CI entities with minimum protections to merit the complete exclusion of these commercial entities from the scope of Bill C-26. Furthermore, the Minister should consider imposing a legislative definition for "Economically Sensitive" industries (supply chain entities, operators, suppliers, or purchasers that are fringe-related to CI but may not be captured by the scope of the CI definition from 2009) so that they are equally considered in the broader CI definition framework to ensure that entities can evolve from one category to another based on ever-changing NS threat trends.

While the focus of this paper does not include a complete legal analysis on the merits of the Government to enact legislation related to other sectors that are not federally regulated, it is important to note that the Government has jurisdiction to regulate other CI sectors based on its powers to legislate matters of NS under the *Constitution Act, 1867*, even if they are not federally

---

[63] Under the *CCPSA*, a "Cyber Security Incident" is an "incident, including an act, omission or circumstance, that interferes or may interfere with the continuity or security of a vital service system; or the confidentiality, integrity or availability of the critical cyber system".
[64] *Supra* note 7, art 9.
[65] Critical 5 (Australia et al.), "Forging a Common Understanding for Critical Infrastructure" (March 2014), online (pdf): *Government of Canada* <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-frgng-cmmn-ndrstndng-crtcalnfrstrctr/index-en.aspx>.

regulated sectors, under their residual "Peace, Order, and good Government" power under Section 91 or the "Defence" power under subsection 91(7).[66]

Including a Ministerial Directive to Heighten National Security Protections Beyond "Vital Systems"

For this reason, CI organizations that fall beyond the scope of the four previously-mentioned sectors should have the capacity to demonstrate that they need more protection from insider EBTs and threat actors. As such, CI organizations should be encouraged to report NS issues to their regulators. This can be facilitated by expanding the Minister's discretionary powers under the legislation to publish Directives under the *CCSPA* framework. This will add in establishing a formal submission process where regulators provide grounds to substantiate findings that a particular CI industry, and the organizations that fall under their oversight, are deeply impacted by NS threats.

This policy modification would allow CI organizations to provide reasoning, trends, and case study examples, in confidence to the Minister, to demonstrate an organization's merits for requesting to be named as a "Designated Operator" beyond the "Vital Systems" that are currently defined under Bill C-26. This Directive would also include resources, assessments, assistance, and other operational tools that CI entities can leverage to indicate a form of "undue hardship" threshold was reached in experiencing NS threats. Organizations could also point to assets such as access to technology, intellectual property, or operational linkages with vulnerable information, goods, or services linked to CI that benefit from further protection. The Directive would specify Government or resources and tools that are approved as sufficient evidence to indicate high-level threat activity to the Minister, notably to cybersecurity systems. The Canadian Government yields

[66] *Constitution Act, 1867* (UK), 30 & 31 Vict, c 3, s 91, reprinted in RSC 1985, Appendix II, No 5.

access to several insider risk management resources and programs as well as partnerships with foreign and domestic organizations that are interested in advancing Canada's NS framework to improve Canada's economic security and NS.[67] Businesses have demanded to have more access to tools and information to protect themselves, and as such, should be able to demonstrate that they would equally benefit from industry protections such as standardization, information sharing, reporting mechanisms, and other legislative measures to protect themselves from threat actors (both non-state affiliated and State Threat Actors) before a scandal hits the headlines and capital is lost.

For example, the Government's Cyber and Infrastructure Resilience Assessment Programs should be highlighted in the suggested Directive under the *CCSPA* for CI or Economically Sensitive organizations that have out-of-date data on threat activity or have not conducted a cybersecurity assessment.[68] The Insider Risk Assessment Tool[69] and the Critical Infrastructure Directorate resources could equally be referenced.[70] To draw on these examples, the findings of the Assessments can help determine a better risk management approach, how to leverage government support, increase cyber security awareness, and determine how to be more resourceful with time and resources to provide security enhancements.[71] Also, the additional feedback collected from Economically Sensitive organizations could fuel a more expansive and modern definition of CI in 2024. Furthermore, if enough concern is demonstrated by CI regulators, perhaps

---

[67] *Supra* note 34.
[68] Public Safety Canada, "Cyber and Infrastructure Resilience Assessments" (15 November 2023), online: Government of Canada <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-en.aspx>.
[69] Public Safety Canada, "The Insider Risk Assessment Tool", (24 October 2022), online: *Government of Canada* <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/irat-oari-en.aspx>.
[70] Public Safety Canada, "Critical Infrastructure" (27 February 2023), online: *Government of Canada* <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx>.
[71] *Ibid*.

this will garnish the attention of the Minister to take further action with their discretionary powers under the *CCSPA* to address industry NS issues based on the tools provided under the legislation.

Discretionary Decision-Making Powers: Source of Concern?

Due to the judicial review requirements under Bill C-26, any evidence to support a case against the reasonability of the Minister's justification to take an action under a Directive is properly safeguarded.[72] Furthermore, evidence collection from regulators would substantiate any unfounded suspicions of inappropriate decision-making power subject to judicial review. To add, the Minister could choose to welcome public consultations or conduct a Regulatory Impact Analysis to see the specific consequences of this regulatory decision on specific industry clusters in CI or those that may fit with the scope of Economically Sensitive Industries (which would require the Government to define sectors that fit under this framework since Canada has taken a definitive approach to qualifying CI sectors in the past).[73]

National Security Impacts All: Keeping Up Canadian Legislation with Insider Economic-Based Threats

By encouraging a larger number of vulnerable sectors to use government tools to voluntarily provide indicators on the prominence of insider EBT to NS, they become incentivized to engage with the objectives of Bill C-26 and take NS issues into their own hands to the furthest extent possible (based on time, resources, and capital). Furthermore, this gives regulators a reporting mechanism that will allow them to make a case on why the industry they regulate should benefit from the application of Bill C-26 according to the evolving NS landscape (for example: benefiting from information sharing with national security agencies based on the risk of threat to their commercial activities). Notably, many companies may feel better protected if they are

[72] *Supra* note 7, art 15.
[73] *Supra* note 24 at 2.

encouraged to improve their resilience against NS threat activity after experiencing a successful or unsuccessful threat attempt to change their approach going forward.

Experts who have testified before the Committee have voiced their concerns about the problem of excluding certain CI sectors that support the four Vital Services sectors.[74] Indirectly, this legislation has created a two-tier system distinguishing CI from more important sectors deemed as "Vital Services".[75] Threat activity is executed using highly sophisticated systems and processes that are constantly changing and still go undetected by Canada and its allies that arguably have stringent NS, cybersecurity, and insider risk protection systems. Recently, when providing expert testimony before the Committee, it was mentioned that a Chinese Hostile State actor went undetected during a covert operation for nearly nine months in the United States' CI network.[76] Canada and its allies need to improve their understanding of foreign interference activity to grasp Hostile State NS interests, their selection methods of insider EBT gateways, and tracking disruptive interference efforts to ensure that Canada can heighten its response to foreign interference.

Without a doubt, NS threats are not only matters of concern for government agencies, but for businesses, their employees and clients, and families.[77] Economic growth is fundamental to advancing economic, military, and cultural power in a globalized economy.[78] State Threat Actors will stop at no means to gain this advantage. Currently, Canadians and their businesses are caught in the crossfire.

---

[74] House of Commons, Standing Committee on Public Safety and National Security, *Minutes 8 April 2024* (Evidence).
[75] S*upra* note 7, art 2.
[76] *Supra* note 74.
[77] *Supra* note 34.
[78] *Supra* note 34.

Research Conclusions: Canada's Next Steps in Mitigating Insider Economic-Based Threats to National Security

In summary, while this research paper offers a critique of Bill C-26, the consequences of delaying its legislative implementation are substantial and adopting the legislation is an urgent step in protecting Canada from current NS threats.[79] Equally as important, threat experts have commented before the Committee that Bill C-26 will assist in reinstating trust in international partnerships such as the Five Eyes Alliance and cross-border NS state relations.[80]As well, the legislation addresses EBT gateways to minimize future capital loss in Canadian CI businesses that are being targeted by foreign interference.[81]

However, the success of Bill C-26 is largely dependent on how the Minister, as the legislated decision-maker, can be forward-looking in using regulatory tools such as Directives and Guidelines, to quickly adapt and respond to NS threats. The Canadian legislative process is lengthy and subject to the political agenda. It is by considering the wide reach of insider EBT gateways, the current impact of threat activity on CI businesses, and the use of those trends to fuel a tailored and ever-changing response strategy that will make Canada more resilient to NS threats.

With the proposed changes to Bill C-26, Canada will be able to respond to hostile threat activity in a proactive and precautionary manner, which is needed with the current state of NS concerns in the 21st century.

"Economic Security is National Security"[82]

At this time, the best threat and risk mitigation strategies in addressing foreign interference are through awareness and best practices in cybersecurity.[83] Once a broader set of businesses are

---

[79] *Supra* note 74.
[80] Supra note 74.
[81] *Supra* note 74.
[82] *Supra* note 34.
[83] *Supra* note 5 at 11.

correctly deemed as Economically Sensitive, Vital Systems, or CI, can effectively monitor human behaviours and social patterns, identify technological vulnerabilities (and likely capital or insurance vulnerabilities), and adapt their systems based on their resources (and governmental assistance in place), real change to the NS landscape can be achieved.[84] This is why Bill C-26 should be expanded in scope to help Economically Sensitive and CI sectors prepare for the likely expansion of the list of CI and Economically Sensitive entities in the years to come. This will also create an evolutionary definition framework for foreign interference threats that is fluid and will allow for adaptability. In reality, the NS environment has changed drastically and Hostile States, such as Russia and the PRC, plan their foreign interference agenda in the long-term which means that NS strategies need to be current and reflective of threat activity in 2024.[85]

Canada has studied foreign interference activity which has helped the Government understand different groups of threat actors and the level of risk of threat that they pose to NS. Therefore, based on these findings, Canada must continue to give special attention to foreign relations, commercial activity, and threat attacks originating from Hostile & Emerging States such as the PRC, Russia, and Iran among others. By identifying Canada's primary insider EBT gateways to NS (investment & ownership, operational relationships, & malicious personnel) sought after by these States in CI to access NS interests, Canada can better predict and reduce harm to future industry targets of foreign interference, economic espionage and broader EBT activity. This begins with more effective and rapid-response tools such as the Minister providing clear directions to industry and updating legislative definitions to provide sector leaders, and their regulators, with opportunities to protect themselves against NS threats.

---

[84] *Supra* note 5 at 11.
[85] *Supra* note 5 at 8.

In this current day in age, we must come to grips that "economic security is national security" which does not only impact government NS agencies but also innovation institutions, citizens, and the entities that remain at the heart of this research paper, the Canadian businesses conducting commercial activities that provide everyday Canadian life.[86]

[86] *Supra* note 34.

WORKS CITED

LEGISLATION: CANADA

Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 1st Sess, 44th Parl 2, 2021.

Canadian Security Intelligence Act, RSC 1985.

Constitution Act, 1867 (UK), 30 & 31 Vict, c 3, s 91, reprinted in RSC 1985, Appendix II, No 5.

SECONDARY MATERIALS: PARLIAMENTARY & GOVERNMENT DOCUMENTS

Canadian Centre for Cyber Security, "The cyber threat from supply chains" (20 August 2021), online (pdf): *Government of Canada* <https://www.cyber.gc.ca/sites/default/files/cyber-threat-supply-chains-v3-e.pdf>.

Canadian Security Intelligence Service, "CSIS Public Report 2021" (2022), online: *Government of Canada* <https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-2021-public-report.html>.

Cybersecurity Advisory, "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure" (Modified 9 May 2022), online: *Cybersecurity & Infrastructure Security Agency* <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a>.

Financial Transactions and Reports Analysis Centre of Canada & the Financial Intelligence Unit of the Netherlands, "Joint financial intelligence advisory: illegal procurement of dual-use goods by Russian end-users" (Modified 22 March 2024), online: *Government of Canada* <https://fintrac-canafe.canada.ca/notices-avis/avs/2024-02-20-eng>.

Government of Canada, "Canadian Sanctions Related to Iran" (Modified 27 March 2024), online: *Government of Canada* <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/iran.aspx?lang=eng>.

Government of Canada, “Economic-Based Threats to National Security” (11 February 2021), online: *Government of Canada* <https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/07-en.aspx>.

Government of Canada, “National Strategy for Critical Infrastructure*”* (2009), online (pdf): *Government of Canada* <https://www.canada.ca/content/dam/nrcan-rncan/site/critical-minerals/Critical-minerals-strategyDec09.pdf>.

Government of Canada, “Policy Regarding Foreign Investments from State-Owned Enterprises in Critical Minerals under the Investment Canada Act ” (8 March 2022), online: *Government of Canada* <https://ised-isde.canada.ca/site/investment-canada-act/en/policy-regarding-foreign-investments-state-owned-enterprises-critical-minerals-under-investment>.

Government of Canada, “Policy Statement on Foreign Investment Review and the Ukraine Crisis” (8 March 2022), online: *Government of Canada* <https://ised-isde.canada.ca/site/investment-canada-act/en/investment-canada-act/policy-statement-foreign-investment-review-and-ukraine-crisis>.

House of Commons, Standing Committee on Industry, Science and Technology, *Minutes 8 June 2020*, (Evidence).

House of Commons, Standing Committee on Public Safety and National Security, *Minutes 8 April 2024* (Evidence).

National Security and Intelligence Committee of Parliamentarians, “Chapter 2: The Government Response to Foreign Interference – Part 1 Annual Report 2019” (2019), online: *National Security and Intelligence Committee of Parliamentarians (NSICOP)* <https://nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/02-03-en.html>.

Parliament of Canada, "An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts" (Consulted 10 April 2024), online: *Government of Canada* <https://www.parl.ca/legisinfo/en/bill/44-1/c-26>.

Public Safety Canada, "Critical Infrastructure" (27 February 2023), online: *Government of Canada* <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx>.

Public Safety Canada, "Cyber and Infrastructure Resilience Assessments" (15 November 2023), online: Government of Canada <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-en.aspx>.

Public Safety Canada, "Foreign Interference" (24 November 2023), online: *Government of Canada* <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/frgn-ntrfrnc/index-en.aspx>.

Public Safety Canada, "Foreign Interference and Hostile Activities of State Actors" (20 August 2021), online: *Government of Canada* <https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/08-en.aspx>.

Public Safety Canada, "Foreign Interference and Canada" (24 November 2023), online: *Government of Canada* <https://www.canada.ca/en/public-safety-canada/news/2023/11/foreign-interference-and-canada.html>.

Public Safety Canada, "The Insider Risk Assessment Tool" (24 October 2022), online: *Government of Canada* <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/irat-oari-en.aspx>.

Public Safety Canada, "National Cross Sector Forum: 2021 – 2023 Action Plan for Critical Infrastructure" (2021), online (pdf): *Government of Canada* <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/2021-ctn-pln-crtcl-nfrstrctr-en.pdf>.

Public Safety Canada, “Protecting Critical Cyber Systems” (Modified 14 June 2022), online: *Government of Canada* <https://www.canada.ca/en/public-safety-canada/news/2022/06/protecting-critical-cyber-systems.html>.

Royal Canadian Mounted Police, “Hydro-Québec employee charged with espionage” (24 November 2022), online: *Royal Canadian Mounted Police* <https://www.rcmp-grc.gc.ca/en/news/2022/hydro-quebec-employee-charged-espionage>.

Standing Committee on Procedure and House Affairs, “Parliamentary Committee Notes: Procurement Safety” (January 31 2023), online: *Government of Canada* <https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20230929/17-en.aspx>.

SECONDARY MATERIALS: INTERNATIONAL DOCUMENTS

Critical 5 (Australia et al.), “Forging a Common Understanding for Critical Infrastructure” (March 2014), online (pdf): *Government of Canada* <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-frgng-cmmn-ndrstndng-crtcalnfrstrctr/index-en.aspx>.

Federal Bureau of Investigation, “The China Threat” (Consulted 10 April 2024), online: *What We Investigate* <https://www.fbi.gov/investigate/counterintelligence/the-china-threat>.

SECONDARY MATERIALS: ARTICLES

Afsha, Bita & Khorasani, Kash, “Dual Use Technology” (October 2020), Online (PDF): *Concordia University* <https://www.concordia.ca/content/dam/ginacody/research/spnet/Documents/BriefingNotes/EmergingTech-MilitaryApp/BN-19-Emerging-technology-and-military-application-Oct2020.pdf>.

Business Council of Canada, “Economic Security is National Security: The Case for an Integrated Canadian Strategy” (7 September 2023), online: *Business Council of Canada* <https://thebusinesscouncil.ca/report/economic-security-is-national-security/#:~:text=Canada%20faces%20a%20series%20of,and%20co%2Dopted%20academic%20research>.

Ciuriak, Dan & Goff, Patricia “Economic Security and the Changing Global Economy” (2021), online (pdf): *Centre for International Governance Innovation* <https://www.cigionline.org/publications/economic-security-and-the-changing-global-economy/>.

Dabu, Christi “‘Global Concern’: High stakes for Canada to have role in widening U.S.-Iran conflict, experts say” (3 February 2024), online: *CTV News* <https://www.ctvnews.ca/politics/global-concern-high-stakes-for-canada-to-have-role-in-widening-u-s-iran-conflict-experts-say-1.6754630>.

D’Andrea, Andrea “National Defence to probe past contracts awarded to firm now tied to China” (8 December 2022), online: *Global News* <https://globalnews.ca/news/9334471/national-defence-sinclair-technologies-canada-china/>.

Mageau, Jack, “Critical Minerals Securitization and Canada’s China Dilemma” (19 May 2023), online: *University of Alberta* <https://www.ualberta.ca/china-institute/research/analysis-briefs/2023/critical-minerals.html>.

Mojtahedi, Negar & Leffler, Brennan, “‘Far Worse than you can imagine’: How Iran’s regime has ‘spread its tentacles’ in Canada” (11 November 2023), online: *Global News* <https://globalnews.ca/news/10076891/iran-dissidents-threats-canada/>.

Panetta, Alexander, “Iran allegedly hired Canadians to conduct assassinations on U.S. soil, according to indictment” (29 January 2024), online: *Radio Canada* <https://www.canada.ca/content/dam/nrcan-rncan/site/critical-minerals/Critical-minerals-strategyDec09.pdf>.

Pugliese, David, “Russia and China at war with Canada, says Gen. Wayne Eyre” (26 October 2023), online: *Ottawa Citizen* <https://ottawacitizen.com/news/national/defence-watch/russia-and-china-at-war-with-canada-says-gen-wayne-eyre>.

Slobodenjuk, Dimitri et al., “The Evolving Concept of National Security Around the World” (6 December 2023), online: *Global Competition Review* <https://globalcompetitionreview.com/guide/foreign-direct-investment-regulation-guide/third-edition/article/the-evolving-concept-of-national-security-around-the-world>.

Tunney, Catherine, “Canada a ‘high-priority’ target for Chinese interference, CSIS doc tells Hague inquiry” (1 February 2024), online: *CBC* <https://www.cbc.ca/news/politics/foreign-interference-inquiry-vigneault-cse-pco-1.7100577#:~:text=%22PRC%20%5Bforeign%20interference%5D%20activity,assessment%20by%20the%20Canadian%20Security>.

Canadian Press, “Ex-Ontario Power Generation employee arrested for alleged security breach involving foreign group” (20 February 2024), online: *CBC News* <https://www.cbc.ca/news/canada/toronto/opg-employee-alleged-security-rcmp-1.7120449>.

Canadian Press, “Former Hydro-Québec employee who is accused of spying for China pleads not guilty to new charges” (6 April 2024), online: *CBC News* <https://www.cbc.ca/news/canada/montreal/former-hydro-quebec-employee-accused-spying-china-1.7165886>.

Tunney, Catherine & Rayecraft, Richard “Canada bans Chinese tech giant Huawei from 5G network” (19 May 2022), online: *CBC News* <https://www.cbc.ca/news/politics/huawei-5g-decision-1.6310839#:~:text=Canada%20bans%20Huawei%20from%20telecom%20networks%20after%20years%20of%20delay,-2%20years%20ago&text=%22This%20has%20never%20been%20about,ban%20Huawei%20from%20telecommunication%20networks>.

SECONDARY MATERIALS: BOOKS

Forcese, Craig & West, Leah, National Security Law, 2nd ed (Toronto: Irwin Law, 2021).