COUNTERING FOREIGN INTERFERENCE IN INDUSTRY AND TECHNOLOGY IN CANADA

Executive Summary

- David Vigneault, Director of CSIS, in the 2022 Public Report, highlighted **foreign interference pervades** Canada across political, social, economic, and technological domains, directly impacting national security. Foreign interference in the form of **industrial and economic espionage**, especially in technology and intellectual property, has a detrimental impact on Canada's strategic advantage and economic benefits. The Canadian government and institutions, including corporations and academia, should **strategically step-up efforts and strengthen policies** to prevent industrial and economic espionage.
- Economic espionage cases date back decades, including the 1990s **Nortel hack** by parties from the People's Republic of China (PRC), attributing to the downfall of Nortel which once had a market capitalization of CAD 380 billion—representing one-third of the Toronto Stock Exchange's market capitalization at its peak. Other incidents involve Qing Huang of **Lloyd's Register** reviewing Canadian military vessel plans **passing trade secrets** to PRC, cross-border **cyber-espionage** in **aerospace**, **infiltration** in **scientific research** (e.g., National Microbiology Laboratory), and technology infiltration in industries like **telecom** (e.g., **Sinclair Technologies**) and **security** (e.g., **Nuctech**). Limited economic espionage cases were charged under Canada's Security of Information Act until Yuesheng Wang's 2022 arrest for **trade secret theft** at **Hydro-Québec**.
- In terms of research and academia, PRC conducts industrial and technology interference under the **Thousand Talents Plan**. PRC enacted the **National Intelligence Law in 2017** stipulating that PRC nationals abroad are also subject to PRC law to gather intelligence from overseas countries, such as Canada, raising concerns of **espionage activities**. Corporations, research institutes, and universities with expertise in the fields of **advanced technologies and innovation**, such as Information and Communications, Health and Life Sciences, Advanced Manufacturing, Natural Resources and Energy, will likely be **targeted**.
- To protect Canada's valuable growth and competitive advantages, a **three-pronged approach** is recommended to counter the growing threats of economic and technological espionage of **ALL adversarial foreign states**:
    1. **Regulatory Enhancement**:
        a. *Expedite the legislation of the **Foreign Influence Registry Act***
        b. *Enact a **federal Canada Trade Secrets Act** to facilitate prosecution proceedings and ensure consistency across provinces*
    2. **Strengthening Institutional security**:
        a. *For corporations: Enhance internal **cybersecurity measures** and guard against insider threats through **robust employee vetting** processes*
        b. *For universities and academic institutions: **Tighten research evaluation** processes, following national security guidelines for research partnership risk assessments*
    3. **Scrutinizing Access to Advanced Technologies**:
        a. ***Restrict access** to selected research and technologies to prevent their study, investment, or acquisition by malign foreign states*
        b. *Initiate a **committee study** to assess our effectiveness in reviewing foreign investments and whether we have a broad enough mandate under the **Investment Canada Act** to review transactions on national security grounds*

Background

According to David Vigneault, Director of the Canadian Security Intelligence Service (CSIS), in the CSIS Public Report 2022[1], foreign interference in Canada targets aspects such as sovereignty, democratic institutions, prosperity, and communities. Foreign states, in pursuit of economic interests, are undermining Canadian innovation and industry, often by exploiting open academic and research entities. The Chinese Communist Party (CCP) exhibits aggression not only through support for Russia's Ukraine invasion but also via hostage diplomacy, foreign interference, espionage, and disinformation within Canada.

Foreign interference pervades Canada across political, social, economic, and technological domains, directly impacting national security. Recently, most of the public attention has focused on political interference (such as interference in Canada's elections, spying on and targeting MPs), and social interference (including secret police operations, spying on, and threatening Canadian residents). The Canadian government and institutions, including corporations and academia, should strategically step up efforts and strengthen policies to prevent foreign interference, particularly in the form of industrial and economic espionage, notably in technology and intellectual property. These measures should extend to all adversarial foreign states, not exclusively the People's Republic of China (PRC).

Scope of Interference

Industrial and economic espionage have a detrimental impact on Canada's strategic advantage and economic benefits. Over the past two decades, various espionage and interference cases have come to light. Notable instances include Chinese hacking that led to Nortel's downfall and Huawei's rise, and the arrest of Yuesheng Wang from Hydro-Québec by the RCMP for trade secret theft. Notably, limited economic espionage cases have been charged under Canada's Security of Information Act.

Cases of Foreign Interference in Industry and Technology:

Case 1: *Hydro-Québec – Economic Espionage in the Power Industry, 2022*

Hydro-Québec employee, Yuesheng Wang, was arrested by the RCMP for obtaining trade secrets "to benefit the People's Republic of China, to the detriment of Canada's economic interests"[2] in 2022. The RCMP identified Wang's actions as a foreign interference attempt, citing Hydro-Québec's role as "critical infrastructure" and "strategic interest to be protected."[3] Wang had spent six years working for Hydro-Québec, during which time he conducted research into battery materials for the utility's Centre of Excellence in Transportation Electrification and Energy Storage.[4] Charges against Wang include obtaining trade secrets, unauthorized computer use, trade secret fraud, and breach of trust by a public officer – marking the first time that the economic espionage charge under the Security of Information Act had been laid in Canada.[5]

---

[1] CSIS Public Report 2022, Government of Canada. Online source: https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-public-report-2022/message-from-director.html

[2] RCMP, 2022. "Hydro-Québec employee charged with espionage," Government of Canada.

[3] Ibid.

[4] Freeze, McGee, Andrew-Gee, 2022. "RCMP lays historic first charge of economic espionage against former Hydro-Québec researcher," Globe and Mail. Online source: https://www.theglobeandmail.com/amp/canada/article-rcmp-china-espionage-quebec/

[5] Lowrie, Morgan, 2022. "RCMP arrest Hydro-Québec employee suspected of spying for China," Montreal Gazette.

Case 2: ***National Microbiology Laboratory – Potential Infiltration in Scientific Research, 2021***

In 2021, Xiangguo Qiu and her husband, Keding Cheng, were dismissed from their posts as infectious-disease scientists at the National Microbiology Laboratory in Winnipeg for reasons the federal government refuses to disclose.[6] Opposition parties passed an Order of the House demanding that "the Public Health Agency of Canada turn over all unredacted documents related to the firing of scientists Xiangguo Qiu and her husband, Keding Cheng."[7] Both Qiu and Cheng are under RCMP investigation for undisclosed reasons.[8] Qiu has close ties to China, with two patents filed by official agencies in China while she worked as a civil servant in Canada and made frequent and repeated trips to the Wuhan Institute of Virology.[9] The Public Servants Intentions Act prohibits government employees from filing patents outside Canada without the permission of the minister responsible.[10] As of June 2022, whether Qiu and Cheng are in Canada or China remains unclear.[11]

Case 3: ***Sinclair Technologies – Technology Infiltration in the Telecom Industry, 2017-2021***

In 2017, the Liberal government waived the necessity for a formal national security review when Hytera acquired Vancouver-based Norsat International Inc., a company whose patented satellite communications technology was used by Canada and many of its allies, including the US, Ireland, and Taiwan.[12] In the United States, Hytera has been banned from being sold or imported due to national security concerns, and its parent company, Shenzhen Investment Holdings, faces 21 espionage-related offences.[13] Formal national security reviews should be undertaken "when the government decides a deal could be injurious to national security," and would analyze the "potential impact on Canada's defence capabilities and economic interests and investigate the impact on the transfer of proprietary technology outside Canada." However, since 2017, several contracts have been awarded to Sinclair Technologies, a subsidiary of Norsat, including contracts with the RCMP, Fisheries and Oceans Canada, and the Department of National Defence.[14] This includes a $549,637 contract awarded to Sinclair Technologies in 2021 for a radio-frequency filtering system intended to protect the RCMP's land-based radio communications from eavesdropping. The installation for this system is currently underway in Ontario and Saskatchewan.[15]

---

[6] Chase, Steven, and Fife, Robert, 2022. "Special committee of MPs will see secret documents on firing of two Winnipeg infectious disease scientists," Globe and Mail.

[7] Bryden, Joan, and Bronskill, Jim, 2021. "Feds drop court quest to keep documents on scientists' firing under wraps," CTV News.

[8] Blackwell, Tom, 2021. "Fired Winnipeg lab scientist listed as co-inventor on two Chinese government patents," National Post.

[9] Ibid.

[10] Canada, 1985. Public Servants Inventions Act, R.S.C., c. P-32.

[11] Chase, Steven, Fife, Robert, and Vanraes, Shannon, 2022. "Whereabouts of fired Winnipeg scientists at centre of national-security investigation still unclear," Globe and Mail.

[12] Chase, Steven, and Fife, Robert, 2017. "Liberals waive security review for Chinese takeover for high-tech firm," Globe and Mail.

[13] Bergeron-Oliver, Annie, 2022. "RCMP contract awarded to company with ties to Chinese government, feds to review process." CTV News.

[14] Ibid.

[15] Godbout, Marc, and Raycraft, Richard, 2022. "Federal government awarded RCMP contract to firm with ties to China," CBC.

Case 4: ***Nuctech – Technology Infiltration in the Security Industry, 2017-2019***

Public Services and Procurement Canada (PSPC) awarded two contracts to Nuctech, a partially Chinese state-owned security company, with Canada Border Services Agency (CBSA) in 2017 and two more in 2019 for X-ray machines.[16] In 2020, a fifth deal with Nuctech was rejected by Global Affairs Canada due to concerns raised about the company's close ties with the Chinese Communist Party (CCP).[17] The Standing Committee on Government Operations and Estimates recommended in a 2021 report that the government "prohibit Chinese state-owned enterprises, partial state-owned enterprises, including companies receiving undisclosed government subsidies, and technology companies from obtaining federal contracts related to information technology or security equipment or services." However, the government has not responded to this recommendation.[18]

Case 5: ***Cross Border Cyber-Espionage in the Aerospace Industry, 2014***

In August 2014, a Los Angeles grand jury indicted a Chinese national named Su Bin (a.k.a. Stephen Su) for his involvement in a cyber-espionage scheme perpetrated by People's Liberation Army hackers.[19] Bin resided in Canada and was a businessman and entrepreneur who specialized in aviation and aerospace products as the owner of a company named Lode-Tech. Between 2008 and 2014, Bin helped two People's Liberation Army hackers steal more than 630,000 files from Boeing related to the C-17 cargo aircraft. The group also targeted data related to the F-22 and F-35 fighter aircraft. Su Bin instructed the hackers on which individuals, companies, and technologies to target and helped translate the data they obtained from English to Chinese. Bin and his co-conspirators also drafted and distributed reports directly to a department in the PLA's General Staff Headquarters.

By 2014, the U.S. Department of Justice had accumulated enough evidence to convince the Canadian government to arrest the suspect and consider an extradition request. This process, though potentially complicated, was simplified when Su Bin voluntarily waived his rights to the extradition process and agreed to return to the U.S. to face the charges.

[16] CBSA, 2020. "Border Security Contracts with Nuctech," Public Safety Canada.

[17] Cooper, Sam, 2020. "$6.8 million Nuctech deal rejected after security review," Global News.

[18] House of Commons, 2021. Ensuring Robust Security in Federal Purchasing: Report of the Standing Committee on Government Operations and Estimates: 43rd Parliament, 2nd Session. Parliament of Canada.

[19] Office of Special Investigations, 2020. "Cyber espionage for the Chinese government," United States government. Online source: https://www.osi.af.mil/News/Features/Display/Article/2350807/cyber-espionage-for-the-chinese-government/

Case 6: *Lloyd's Register – Economic Espionage in the Shipbuilding Industry, 2013*

Qing Huang was charged under the Security of Information Act for attempting to pass secrets to the Chinese government—an exceptionally rare occurrence in Canada, with only two other such cases since September 11, 2001.[20] Huang worked for a company called Lloyd's Register, where he had been hired by Irving Shipbuilding to review plans for Canadian military vessels. On November 13, 2013, during a meeting with his supervisors, it was clearly communicated that his job was in jeopardy due to certain circumstances. Two days later, Huang downloaded approximately 6,000 files from the internal company network. On November 25, 2013, Huang made two telephone calls to the Chinese embassy in Ottawa. Both calls were recorded by the Canadian Security Intelligence Service. Subsequently, as a result of these calls, the Royal Canadian Mounted Police had an undercover officer posing as a Chinese embassy official meet with Huang. Almost a decade later, the prosecution of the case has been halted, indicating that spy prosecutions are exceedingly difficult and rare in Canada.

Case 7: *Nortel – Economic Espionage in the Telecom Industry, 2004*

Nortel, a telecommunications giant in Canada, fell and filed for bankruptcy in 2009. Prior to the company's failure, a cybersecurity advisor's investigation in 2004 indicated that Nortel was invaded by hackers based in China who stole over 1,400 sensitive intellectual property and internal documents, including Nortel technology, technical papers, directions of various products, sales proposals, pricing, and network design, etc.[21] The hackers used passwords stolen from its top executives. The actual loss of sensitive information could have been much greater, as the investigation indicated that the break-in of Nortel's internal computer network likely began in the 1990s. The Canadian Security Intelligence Service (CSIS) also warned Nortel of Beijing-led human spies. It was cited that the People's Republic of China's attack on Nortel had many facets, from systematic hacking and planting of electronic bugs and spies inside Nortel facilities to the use of Chinese PhD students hired by Nortel to steal research and attempts to compromise Nortel managers using spies from the Chinese Communist Party and People's Liberation Army.[22]

In terms of research and academia, PRC also conducts industrial and technology interference under the Thousand Talents Plan (TTP). This initiative recruits experts, often from the science and tech field, from abroad, leading to claims of espionage[23]. CSIS notes that TTP can be used as a "tool to reward scientists for giving up information or as a way of coercing them to do so," with incentives that

[20] Shull, Aaron, 2022. "Why Espionage Cases Are So Hard to Prosecute," Centre for International Governance Innovation. Online source: https://www.cigionline.org/articles/why-espionage-cases-are-so-hard-to-prosecute/

[21] Blackwell, Tom, 2020. "Exclusive: Did Huawei bring down Nortel? Corporate espionage, theft, and the parallel rise and fall of two telecom giants," National Post. https://nationalpost.com/news/exclusive-did-huawei-bring-down-nortel-corporate-espionage-theft-and-the-parallel-rise-and-fall-of-two-telecom-giants

[22] Cooper, Sam, 2020. "Inside the Chinese military attack on Nortel," Global News. https://globalnews.ca/news/7275588/inside-the-chinese-military-attack-on-nortel/

[23] Fife, Robert and Chase, Steven, 2020. "CSIS warns about China's efforts to recruit Canadian scientists," The Globe and Mail.

include "high salaries, research funds, laboratory space and preferential treatment including medical care."[24] As of August 2020, there are 47 identified talent-recruitment stations in Canada.[25]

PRC enacted the National Intelligence Law in 2017 which allows national intelligence institutions to "request relevant organs, organisations, and citizens provide necessary support, assistance, and cooperation."[26] This law contains provisions that explicitly codifies the practice of individuals and organizations conducting national intelligence work on behalf of the state. Article 7 states that "all organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of," while Article 10 states they may "use the necessary means, tactics, and channels to carry out intelligence efforts, domestically and abroad."[27] This implies that Canada can be impacted by the PRC's efforts to recruit experts, particularly mainland Chinese scientists and researchers residing in Canada, as well as gather intelligence from the country. This situation gives rise to concerns regarding espionage, the sharing of sensitive information, and activities that compromise national security.

Areas of Impact

Quantifying the damage caused by state-sponsored industrial and economic espionage to the Canadian economy is challenging. The downfall and bankruptcy of Nortel, which once had a market capitalization of CAD 380 billion—representing one-third of the Toronto Stock Exchange's market capitalization at its peak[28]—demonstrated how significant the financial loss could be to the economy and individual investors in Canada. Drawing from the U.S. experience, the financial consequences of industrial espionage are substantial. According to Mike Orlando, the director of the National Counterintelligence and Security Center, the annual cost of PRC espionage in the United States alone is estimated at approximately US$600 billion.[29] On average, the FBI initiates a new PRC-related counterintelligence investigation every 12 hours.[30] This scale suggests that the threat to the Canadian economy, as an innovative and technologically advanced country, is considerable moving forward.

As the People's Republic of China faces significant challenges in its economic growth and becomes increasingly aggressive internationally, we can anticipate more economic, industrial, and technology espionage activities in Canada. Corporations, research institutes, and universities with expertise in the fields of advanced technologies and innovation will likely be targeted. These fields[31] include:

- Environment and agriculture: Biotechnology, climate change research and technology, and more.
- Information and communications: Cybersecurity, quantum computing, artificial intelligence, machine learning, and more.

---

[24] CSIS, 2020. "Thousand Talents Plan," Public Safety Canada.

[25] Joske, Alex, 2020. Hunting the phoenix: The Chinese Communist Party's global search for technology and talent. Australian Strategic Policy Institute.

[26] CSIS, 2018. "China's intelligence law and the country's future intelligence competitions," Government of Canada

[27] China Law Translate, 2017. "PRC National Intelligence Law (as amended in 2018)." China Law Translate.

[28] CBC News, 2001. Online source: https://www.cbc.ca/news/business/nortel-briefly-loses-title-as-canada-s-biggest-company-1.269268

[29] Ekran, 2023. "Industrial & Corporate Espionage: What Is It, Cases & Best Prevention Practices". Online source: https://www.ekransystem.com/en/blog/prevent-industrial-espionage

[30] Ibid.

[31] Canada's Innovation Strengths and Priorities – Innovation Expertise in Canada, 2019. Government of Canada. Online source: https://www.tradecommissioner.gc.ca/innovators-innovateurs/strategies.aspx?lang=eng

- Health and life sciences: Biomedical engineering, medical technologies, regenerative medicine, and more.
- Advanced manufacturing: Automation, robotics, nanotechnology, aerospace, and more.
- Natural resources and energy: Bioenergy, fuel cells, nuclear energy, and more.

Recommendations

Not only does the Canadian government need to expedite the legislation of the Foreign Influence Registry Act, a critical starting point for creating transparency around foreign agencies operating in Canada, but we also recommend that the Canadian government adopt a three-pronged approach to counter the growing threats of economic and technological espionage and to protect our valuable growth and competitive advantages. These approaches are as follows:

1. Regulatory Enhancement
2. Strengthening Institutional Security
3. Scrutinizing Access to Advanced Technologies

1. Regulatory Enhancement

Currently, Canada lacks a federal trade secrets act or equivalent statute. Instead, trade secret law relies on common law, while civil law principles are enforced, including torts, breaches of contract, or confidence, in the province of Quebec.[32] Although economic espionage has been a criminal offense in Canada since 2001 under section 19 of the Security of Information Act (SIA), prosecutions under this provision have been limited[33] until the recent Hydro-Québec case. Challenges for prosecution under section 19 of the SIA include:

- The requirement of a "Foreign Economic Entity," which is overly restrictive and makes establishing the necessary relationship between an entity and a foreign government difficult.[34]
- The "Detriment of Canada's Interests" requirement, which is too vague. The misuse of a trade secret must be "to the detriment of Canada's economic interests, international relations, or national defence or security." It remains unclear whether actions in section 3 of the SIA are sufficient to establish detriment to Canada's interests.[35]
- Corporate reluctance to provide information vital to prosecution due to a lack of provisions for preserving trade secret confidentiality during espionage litigation.[36]

We recommend enacting a federal Canada Trade Secrets Act that addresses requirements and provisions to facilitate prosecution proceedings and ensure consistency across provinces.[37] This Act

[32] Malone, Matt, 2021. "Why We Need a Canada Trade Secrets Act," Slaw. Online source: https://www.slaw.ca/2021/11/26/why-we-need-a-canada-trade-secrets-act/
[33] Ibid.
[34] LaRoche, Colin, 2020. "A new way to prosecute Economic Espionage? Section 19 of the Security of Information Act, and the new "Trade Secrets" Offence," INTREPID. Online source: https://www.intrepidpodcast.com/blog/2020/11/18/a-new-way-to-prosecute-economic-espionage-section-19-of-the-security-of-information-act-and-the-new-trade-secrets-offence
[35] Ibid.
[36] Ibid.
[37] Dafniotis, Panagiota, 2022. "Trade Secret Protection and Remedies in Canada," Dentons. Online source: https://www.dentons.com/en/insights/articles/2022/february/25/trade-secret-protection-and-remedies-in-canada

should also better protect trade secret information during litigation and introduce stronger penalties and criminal codes (such as treason) to effectively deter espionage activities.

2. Strengthening Institutional Security

While regulatory improvements and enhancing the Trade Secrets Act can make prosecuting and deterring economic and technological espionage more effective, Canada remains vulnerable to foreign state espionage if corporations, research institutes, and universities do not strengthen their measures to safeguard technological know-how, research assets, and trade secrets against cyberattacks, infiltration, and insider threats posed by foreign spies masquerading as regular employees.[38]

For corporations, we recommend establishing a public-private partnership program aimed at educating and enhancing corporations' internal policies and capabilities to bolster cybersecurity and guard against insider threats through robust employee vetting processes. This could involve a strategic review of current security capabilities and vetting processes across companies and research institutions in advanced technology areas.[39]

For universities and academic institutions, each university's research office should tighten its evaluation process to prevent potential espionage activities by:

- Adopting a similar evaluation standard to that of the Research Security Center for assessing federal grant applications.[40] Depending on the nature and partners of the research contract, professors should be required to conduct research partnership risk assessments following national security guidelines.[41]
- Providing sufficient training to research officers to enable informed decisions.[42]
- Offering periodic, compulsory, and concise training to professors in sensitive areas to raise their awareness of potential foreign interference. The "Safeguarding Science" program by Public Safety can be made more active for this purpose.[43]

3. Scrutinizing Access to Advanced Technologies

As emphasized by the former head of CSIS, Richard Fadden, given the People's Republic of China (PRC)'s aggressive acquisition of intellectual property from other countries, Canada must consider restricting access to certain research and technologies to prevent their study, investment, or acquisition.[44] If Western countries act collectively to prevent the outflow of advanced and/or military technology to PRC, there will be less backlash for any individual nation.

---

[38] Ekran, 2023. "Industrial & Corporate Espionage: What Is It, Cases & Best Prevention Practices". Online source: https://www.ekransystem.com/en/blog/prevent-industrial-espionage

[39] Ibid.

[40] Academic expert interview.

[41] For example, National Security Guidelines for Research Partnerships Risk Assessment Form to assess risk of exposure to espionage activities: https://ncc-cnc.ca/wp-content/uploads/2023/05/Template-J-1-National-Security-Guidelines-for-Research-Partnerships-Risk-Assessment-Form-.pdf, Innovation, Science and Economic Development Canada.

[42] Academic expert interview.

[43] Ibid.

[44] Dyer, Evan, 2020. "Experts call on Canadian universities to close off China's access to sensitive research," CBC News. Online source: https://www.cbc.ca/news/politics/china-canada-universities-research-waterloo-military-technology-1.5723846

We understand that this policy is sensitive and should avoid being perceived as discriminatory. Therefore, we recommend rigorous immigration vetting for individuals from malign foreign states, and tightening the vetting policy and process for investment, study visas, and work permits in advanced technology areas to mitigate infiltration by adversarial foreign states. For instance,

- The Canadian government should enhance the foreign investment screening process. While the government occasionally halts acquisition activities related to natural resources, it should extend this evaluation process to acquisitions involving companies possessing sensitive data or advanced technologies.[45] We also strongly recommend that the Canadian government initiate a committee study to assess our effectiveness in reviewing foreign investments, especially those from adversarial foreign states, and whether we have a broad enough mandate under the Investment Canada Act to review transactions on national security grounds. This committee study should advise the Canadian government on whether to set up and authorize an inter-ministerial committee to review transactions involving foreign investment in Canada and certain real estate transactions by foreign persons. The goal is to determine the effect of such transactions on the national security of Canada and to ban investments from adversarial foreign states that raise national security concerns.

- The China Scholarship Council (CSC) is a research funding agency in the PRC. Every year, numerous CSC-sponsored scholars and students visit Canadian universities, gaining access to various research labs. However, our understanding is that CSC-sponsored students must sign a document declaring loyalty to the Chinese government before receiving grants. In cases where they do not adhere to this principle or fail to comply with instructions, their families in the PRC are obligated to reimburse the CSC scholarships to the PRC government. The amount involved is substantial, effectively holding the families of CSC scholarship recipients hostage. Consequently, there is an elevated risk of espionage activities if these individuals work in sensitive areas.[46] We recommend that the Canadian government implement a program to:
    - ➢ Strengthen the vetting process during the visa application stage, especially when Canadian professors (hosts) are involved in sensitive areas.[47]
    - ➢ Raise awareness among professors and academia, particularly those in sensitive areas, about this matter through regular training and communication initiatives.[48]

- As mentioned earlier, PRC enacted the National Intelligence Law in 2017. This law stipulates that PRC nationals abroad are also subject to PRC law when it comes to gathering intelligence from overseas countries, such as Canada. This has raised concerns about espionage, the sharing of sensitive information, and activities that compromise the national security of these countries. The Canadian government should consider policies to:
    - ➢ Prohibit individuals from ALL adversarial foreign states, not just PRC, from using study visas or work permits to come to Canada for study or employment in selected fields of advanced technologies and innovation.
    - ➢ Prohibit Canadian citizens and permanent residents who also hold nationality from adversarial foreign states from studying or obtaining employment in selected fields of advanced technologies and innovation.

[45] Academic expert interview.
[46] Ibid.
[47] Ibid.
[48] Ibid.

In summary, foreign interference in the form of industrial and economic espionage poses a serious national security issue. The aforementioned measures necessitate cross-ministerial efforts and collaboration across the jurisdictions of Innovation, Science and Industry, Justice, Public Safety, and Immigration and Citizenship. Given the significant stakes at hand, we urge the Canadian government to take orchestrated actions to study, develop, and implement timely measures to better protect Canada from foreign interference.