Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

Academic Outreach and Stakeholder Engagement

Guidance for Entities Responding to COVID-19

13 May 2020

Introduction

- CSIS is continuing our work during the pandemic, and this includes addressing the threat of foreign interference and espionage. We are working closely with partners, within and outside Canada, to help safeguard Canada's contribution to global efforts to protect humanity from COVID-19 and to address threats to Canadian interests and prosperity.
- Your efforts and your research on matters related to COVID-19 may make you a target for those kinds of activities by hostile foreign state actors.
- Canada has an abundance of natural resources, advanced technology, human talent, and expertise. We are world leaders in many sectors. We have powerful allies with whom we enjoy close economic, security, and defence relationships. We are a wealthy and highly developed nation. All of that makes us a target.
- Hostile foreign intelligence services or people who are working with the tacit or explicit support of foreign states gather political, economic, commercial, or military information through clandestine means here in Canada.

"While the threats of espionage and foreign interference are nothing new, a number of factors have combined during this time to increase the risks to Canadian interests. On the Canadian side, these include a surge in innovative research and development within Canada (a significant amount of which is publicly funded); increased use of remote-working arrangements; and expansion of international partnerships. On the foreign threat actor side, CSIS is seeing rapid evolution in the nature and volume of threat activities and their focus on new targets in Canada."

- CSIS is conducting outreach to support entities in protecting their research and development, intellectual property or business interests by increasing their awareness of this threat and the steps they can take to protect themselves.

- Please contact CSIS with any questions or concerns. You can find our contact information here: https://www.canada.ca/en/security-intelligence-service/corporate/contact-us.html
- If you have questions related specifically to a cyber incident or cyber security, we would invite you to contact our partners at the Canadian Centre for Cyber Security. You can find its contact information here: https://cyber.gc.ca/en/contact-us

Targeted Sectors for Foreign Espionage

- Understandably, the biopharmaceutical and healthcare sectors are at a significantly high risk at this time as many countries are accelerating their COVID-19 research and development to support the pandemic response.
- While many researchers and development teams are invested in working transparently and collaboratively across borders towards a common objective, there are those who, unfortunately, seek to exploit this sharing for their own strategic or economic advantage.
- It is important to be aware however that these are not the only sectors of the economy being targeted at this time.

"Sectors such as artificial intelligence, quantum computing, nanotechnology, big data analytics, next gen and manufacturing involved in the COVID-19 response effort also pose an attractive target for foreign espionage."

- CSIS is particularly concerned about this threat in relation to the state-sponsored activities of hostile states secretly seeking strategic or competitive advantage.
- Certain governments are prepared to use both licit and illicit means to obtain goods and technology to advance their own interests. Licit means can include purchase and foreign investment. Illicit means can include theft of goods and technology through a variety of means such as unauthorized exports, intangible technology transfer, cyber-attacks, and use of human sources and assets.

Four Gates

- CSIS has developed the framework of the "Four Gates" of economic security to understand and explain these threats.
- Sensitive and proprietary technology, know-how and assets can be accessed in any of four ways: attacks on knowledge, investments, imports/exports, and licenses.

Attacks on Knowledge

- The exposure of sensitive Canadian knowledge – such as research, intellectual property, as well as personal and corporate data – can happen in a number of ways including cyber-espionage, the use of insider threats (compromising an internal network or transferring proprietary technology), and intangible technology transfer through, for example, research collaboration.
- "Cyberspies" and insider threat actors have received a lot of public attention in the past for their involvement in attacks on knowledge, but another less well-known type of actor is the non-traditional intelligence collector.
- Put simply, this refers to people without formal intelligence training but with a particular subject matter expertise such as businesspeople, scientists, researchers, and even students. These individuals know what is valuable and they are able to operate in business and research environments without raising suspicions.
- Non-traditional intelligence collectors may have no premeditated intent to cause harm to your organization or Canada. However, they can also be vulnerable to state demands if they return to an authoritarian country with a disregard for intellectual property rights and patents. If that foreign state becomes aware those individuals have access to your valuable information, it may compel them to hand over your intellectual property with full legal backing to force their assistance.

"Beyond research and intellectual property, Canadians' financial and healthcare information may also be targeted by threat actors."

- This type of information holds intimate details about a person or organization, including their potential vulnerabilities, that a foreign government may exploit in support of hostile activities such as espionage, sabotage or disruption.
- You may unwittingly invite these non-traditional collectors into your front door, as you pursue business arrangements or R&D collaborations.

Investment

- Canada's stable economy and sound financial system make it an attractive destination for foreign investment. A small proportion of that investment poses a threat to Canada's national security and prosperity.

- In the current context, foreign governments may seek to invest to gain access and control of sensitive technology and know-how. Investment can also provide threat actors with access to or control over Canadian critical infrastructure, including essential supply chains.

"This pandemic has highlighted the importance of securing supply chains for vital public health goods. CSIS wants to ensure that foreign investment does not facilitate state-sponsored efforts to gain access and control over goods which are essential to the global public health response."

- By investing in your company, threat actors may gain access to everything you know and everything you own.
- The risks of foreign investment which is aimed at acquisition of strategic Canadian goods, technology, and intellectual property are real. If you receive any unexpected offers in the coming days and weeks, please give this careful consideration and reach out to CSIS with any concerns.

"It is important that you know that what appears to be a lucrative foreign investment may have hidden strings – and consequences – attached."

Imports & Exports

- The purchase and export of advanced technologies, which can then be copied or reverse-engineered, is a well-known national security concern. However, in the current context of COVID-19, a growing concern is the risk of targeted attacks on supply chains which would have a severe impact on the government's ability to ensure the safety and security of Canadians and of Canada's ability to contribute to global health innovation.
- Medicinal ingredients, personal protective equipment, and other medical supplies are examples of essential items that, if denied to Canada due to compromised supply chains, could negatively impact Canada's COVID-19 response.
- CSIS is also concerned about the import of foreign goods which are sub-standard and/or fraudulent. If those are health goods, it places Canadian lives at risk. The RCMP can advise and help you with those concerns.

Licences

- Certain licenses may confer privileged rights or access to physical spaces or sensitive data, which may be exploited to cause harm to Canada and Canadians. Typical examples of such licences include visas, patents, industrial certifications, and distribution agreements.

- Often the licences are not the objective themselves, but rather a means to the threat actor's ultimate goal, such as access to Canadian data, critical infrastructure, or the right to enter Canada.
- In the context of COVID-19, examples of licences that may be targeted include pharmaceutical patents, biotechnology patents, authorizations to use specific medicines or procedures.

> ***"Your intellectual property may be exposed to theft if you enter into licensing or other contractual arrangements with foreign partners, in an expectation that they will abide by Canadian laws and norms."***

The Threat is Real; But You Are Not Alone

- Why should you care about these threats?
    - First, this espionage threatens the very livelihood of your business or institution and jeopardizes Canadian interests and prosperity. For the research community, it can mean that important scientific breakthroughs may be transferred to countries unwilling to share the benefits, or that Canada's contribution to global public health efforts is compromised.

> ***"Espionage can extinguish the prospects of any single business – in the aggregate, it can pose challenges to entire sectors, placing Canada at a long-term disadvantage that will erode prosperity."***

    - Worse, in the context of COVID-19 pandemic, some of this threat activity may create new risks that jeopardize Canadians' health and safety.
- CSIS is available to hear your concerns and offer support. Please be aware:
    - Threat actors may try all four gates, but only need to succeed in one to do significant harm to you and Canadian interests;
    - Nationality is not an accurate indicator of whether an individual or organization will be a good partner or employee or may pose a threat;
    - When entering into partnerships, it is vital that you understand who controls your potential partner and the goods or technology you create, and who will benefit from your activities;
    - If you are receiving Government of Canada funding verify if there are particular limitations or requirements with regard to intellectual property or research integrity that must be adhered to; and,

- Threats come in all sizes and dollar values. Even if you are small, your work may be of great interest. Your work may a critical piece of a bigger puzzle.

- CSIS has a Canada-wide presence. Should a situation arise, please contact one of our regional offices to discuss any potential threat activity: https://www.canada.ca/en/security-intelligence-service/corporate/contact-us.html

"CSIS is joined in this effort by partners in other parts of the Government of Canada. We are working together to detect, deter and respond to these threats on a daily basis to keep Canada safe and prosperous."